

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 23 - Trattamento di dati relativi alla gestione delle biblioteche e dei centri di documentazione (Obbligo DPIA)
Settore	Settore 2 - Servizi alla Persona
Servizio	2.2 - Biblioteca Civica - Cultura
Ufficio: denominazione e punti di contatto	Biblioteca Civica
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	Sistema Bibliotecario Urbano e cultura Biblioteca Civica "Renzo Deaglio" - Piazza Airaldi e Durante 7

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gestione prestito locale.

Gestione prestito interbibliotecario

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 37 - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati
Settore	Settore 2 - Servizi alla Persona
Servizio	2.2 - Biblioteca Civica - Cultura
Ufficio: denominazione e punti di contatto	Biblioteca Civica
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Concessione contributi per manifestazioni

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 39 - Trattamento di dati relativi alle attivita' ricreative, di promozione dei giovani.
Settore	Settore 2 - Servizi alla Persona
Servizio	2.2 - Biblioteca Civica - Cultura
Ufficio: denominazione e punti di contatto	Biblioteca Civica
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	Sistema Bibliotecario Urbano e cultura Biblioteca Civica "Renzo Deaglio" - Piazza Airaldi e Durante 7

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio manifestazioni ed eventi

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
Settore	Amministratori
Servizio	Amministratori
Ufficio: denominazione e punti di contatto	Consiglio comunale e commissioni consiliari
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Istituzione commissioni permanenti, temporanee o speciali

Istituzione commissioni permanenti, temporanee o speciali

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali
Settore	Amministratori
Servizio	Amministratori
Ufficio: denominazione e punti di contatto	Consiglio comunale e commissioni consiliari
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare,

	con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Procedure di valutazione relative all'analisi dell'impatto della regolamentazione (AIR) ai sensi dell'art.14, comma 1, della legge 28 novembre 2005, n. 246

Mozioni, ordini del giorno, risoluzioni, interrogazioni ed interpellanze

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
Settore	Amministratori
Servizio	Giunta Comunale
Ufficio: denominazione e punti di contatto	Giunta Comunale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Nomine e affidamenti incarichi per prestazioni o servizi per i quali le determinazioni siano fondate su rapporti fiduciari

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 49 - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento
Settore	Amministratori
Servizio	Giunta Comunale
Ufficio: denominazione e punti di contatto	Giunta Comunale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Autorizzazione al ricorso a transazioni e altri rimedi di risoluzione delle controversie alternativi a quelli giurisdizionali

Accordi integrativi o sostitutivi del provvedimento

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Amministratori
Servizio	Giunta Comunale
Ufficio: denominazione e punti di contatto	Giunta Comunale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Convenzioni con associazioni e altri enti di diritto privato non di competenza del Consiglio

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale contrattualizzato presso il Comune (Obbligo DPIA)
Settore	Amministratori
Servizio	Sindaco
Ufficio: denominazione e punti di contatto	Sindaco
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Nomina Segretario generale

Attribuzione e revoca incarichi al personale dirigente

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
Settore	Amministratori
Servizio	Sindaco
Ufficio: denominazione e punti di contatto	Sindaco
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Nomine e affidamenti incarichi per prestazioni o servizi per i quali le determinazioni siano fondate su rapporti fiduciari

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 36 - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti.
Settore	Amministratori
Servizio	Sindaco
Ufficio: denominazione e punti di contatto	Sindaco
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli

	elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Ordinanze in qualita' di Ufficiale di governo

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 49 - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento
Settore	Amministratori
Servizio	Sindaco
Ufficio: denominazione e punti di contatto	Sindaco
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accordi integrativi o sostitutivi del provvedimento

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 51 -- Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato (Obbligo DPIA)
Settore	Amministratori
Servizio	Sindaco
Ufficio: denominazione e punti di contatto	Sindaco
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accesso art. 43, co. 2 del T.U.E.L. da parte dei consiglieri

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 29 - Trattamento di dati relativi al rilascio delle licenze e autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza
Settore	TUTTI I SETTORI - ATTIVITA' TRASVERSALE
Servizio	2.5 - Servizio Commercio (SUAP)
Ufficio: denominazione e punti di contatto	Sportello Unico Attivita' Produttive
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di

	climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei

	dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Segnalazione certificata di inizio attivita' (SCIA) per l'esercizio attivita' di lavanderia
 Segnalazione certificata di inizio attivita' (SCIA) per ascensori
 Commercio su aree pubbliche con posteggio in mercati - Autorizzazione
 Commercio itinerante su aree pubbliche - Autorizzazione
 Segnalazione certificata di inizio attivita' (SCIA) per l'esercizio attivita' di Acconciatore, Estetista, Esecuzione tatuaggi e piercing
 Segnalazione certificata di inizio attivita' (SCIA) per l'esercizio attivita' circhi
 Segnalazione certificata di inizio attivita' (SCIA) per esercizi di commercio al dettaglio - media struttura di vendita con superficie fino a mq. 1.500
 Segnalazione certificata di inizio attivita' (SCIA) per attivita' ricettive extra alberghiere: attivita' agriturismo- Bed and Breakfast, affittacamere.
 Trasferimento di residenza di titolare in autorizzazione per l'attivita' di commercio al dettaglio su aree pubbliche in forma itinerante e richiesta nuova - Autorizzazione
 Segnalazione certificata di inizio attivita' (SCIA): esercizio di somministrazione di alimenti e bevande - nuova apertura
 Segnalazione certificata di inizio attivita' (SCIA): esercizio di somministrazione di alimenti e bevande - subingresso
 Segnalazione certificata di inizio attivita' (SCIA): esercizio di somministrazione di alimenti e bevande - trasferimento
 Segnalazione certificata di inizio attivita' (SCIA): esercizio di somministrazione in circolo privato
 Segnalazione certificata di inizio attivita' (SCIA): esercizio di somministrazione temporanea di alimenti e bevande in occasione di manifestazioni
 Noleggio di veicoli con conducente - Autorizzazione
 Noleggio di veicoli senza conducente - Autorizzazione
 Pubblica sicurezza: falo' tradizionale - Autorizzazione -Accensione luminarie e similari.
 Pubblica sicurezza: Lotteria, tombola e pesca di beneficenza - Autorizzazione
 Segnalazione certificata di inizio attivita' (SCIA) per l'esercizio attivita' ricettive complementari: case vacanze
 Pubblica sicurezza: mestiere di fochino - Autorizzazione
 Pubblica sicurezza: rimessa veicoli - Autorizzazione
 Pubblica sicurezza: strumenti da punta e da taglio - Autorizzazione
 Rivendite di quotidiani e periodici - Autorizzazione
 Commercio itinerante su aree pubbliche e su posteggio - subingresso - Autorizzazione

Taxi - Autorizzazione

Segnalazione certificata di inizio attivita' (SCIA): commercio elettronico, vendita per corrispondenza, televisione

Segnalazione certificata di inizio attivita' (SCIA): vendita al dettaglio a domicilio

Manifestazioni fieristiche-Fiere - Autorizzazione

Segnalazione certificata di inizio attivita' (SCIA) per l'esercizio attivita' di giochi leciti e videogiochi

Pubblica sicurezza: istruttore / direttore di tiro a segno - Autorizzazione

Segnalazione certificata di inizio attivita' (SCIA): vendita diretta da parte dei produttori agricoli

Attivita' funebre - Autorizzazione

Segnalazione certificata di inizio attivita' (SCIA) per l'esercizio attivita' ricettive complementari: strutture ricettive all'aria aperta - campeggi

Segnalazione certificata di inizio attivita'(SCIA): commercio all'ingrosso nel settore alimentare e non alimentare

Vendita ambulante di strumenti da punta e da taglio - Autorizzazione

Segnalazione certificata di inizio attivita' (SCIA): somministrazione di alimenti e bevande tramite mense, ristorazione collettiva nell'ambito di case di riposo, ospedali, scuole, caserme, comunita' religiose

Segnalazione certificata di inizio attivita' (SCIA): somministrazione di alimenti e bevande nell'ambito di altre attivita' quali sale giochi, sale scommesse autorizzate ai sensi del TULPS (Testo unico leggi di pubblica sicurezza)

Segnalazione certificata di inizio attivita' (SCIA) attivita' artigianali in genere, compresi i laboratori di produzione, di trasformazione e/o confezionamento con/senza attivita' di vendita diretta al consumatore finale

Segnalazione certificata di inizio attivita' (SCIA): somministrazione di alimenti e bevande nell'ambito di musei, teatri, sale da concerti

Segnalazione certificata di inizio attivita' (SCIA): somministrazione di alimenti e bevande nell'ambito di altre attivita' quali sale da ballo, locali notturni, stabilimenti balneari, impianti sportivi

Segnalazione certificata di inizio attivita' (SCIA): commercio di prodotti agricoli e zootecnici, mangimi, prodotti di origine minerale e chimico industriali destinati all'alimentazione animale

Segnalazione certificata di inizio attivita' (SCIA)

Distributori di carburanti - Autorizzazione

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 29 - Trattamento di dati relativi al rilascio delle licenze e autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza
Settore	Settore 4 - Tecnico
Servizio	4.1 - Servizio Urbanistica - Edilizia Privata - SUAP
Ufficio: denominazione e punti di contatto	Sportello Unico Attivita' Produttive
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di

	climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei

	dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio di parafarmacia

Distributori di carburanti - Autorizzazione

Esercizi di commercio al dettaglio grandi strutture di vendita - Autorizzazione

Esercizi pubblici: apertura e trasferimento di pubblico esercizio in zona sottoposta a tutela - Autorizzazione

Pubblica sicurezza: fuochi d'artificio - Autorizzazione

Segnalazione certificata di inizio attivita' (SCIA)

Segnalazione certificata di inizio attivita' (SCIA): stabilimenti industriali

Segnalazione certificata di inizio attivita' (SCIA): variazione della superficie degli esercizi pubblici di somministrazione alimenti e bevande

Rilascio autorizzazioni

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale contrattualizzato presso il Comune (Obbligo DPIA)
Settore	TUTTI I SETTORI - ATTIVITA' TRASVERSALE
Servizio	Tutti i Servizi - Attivita' trasversale
Ufficio: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Assunzioni interinali

Piani formativi e corsi di formazione

Conferimento di incarichi di collaborazione, studio e ricerca nonché di consulenza a soggetti estranei all'amministrazione

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 30 - Trattamento di dati relativi all'attivita' di consulenza giuridica, nonche' al patrocinio ed alla difesa in giudizio dell'amministrazione nonche' alla consulenza e copertura assicurativa in caso di responsabilita' civile verso terzi dell'amministrazione
Settore	TUTTI I SETTORI - ATTIVITA' TRASVERSALE
Servizio	Tutti i Servizi - Attivita' trasversale
Ufficio: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Controversie e contenziosi esterni ed interni, citazioni, costituzioni in giudizio, e conseguente nomina dei difensori e consulenti

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 35 - Trattamento di dati relativi agli istituti di democrazia diretta
Settore	TUTTI I SETTORI - ATTIVITA' TRASVERSALE
Servizio	Tutti i Servizi - Attivita' trasversale
Ufficio: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Attivita' riguardante gli istituti di democrazia diretta

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	TUTTI I SETTORI - ATTIVITA' TRASVERSALE
Servizio	Tutti i Servizi - Attivita' trasversale
Ufficio: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamenti di entrata

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 43 - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche (Obbligo DPIA)
Settore	TUTTI I SETTORI - ATTIVITA' TRASVERSALE
Servizio	Tutti i Servizi - Attivita' trasversale
Ufficio: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare,

	con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Liquidazione fatture

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 48 - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'
Settore	TUTTI I SETTORI - ATTIVITA' TRASVERSALE
Servizio	Tutti i Servizi - Attivita' trasversale
Ufficio: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Segnalazione-Esposto

Segnalazioni di illecito

Gestione del rischio violazione sicurezza del trattamento dei dati personali - DPIA

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	TUTTI I SETTORI - ATTIVITA' TRASVERSALE
Servizio	Tutti i Servizi - Attivita' trasversale
Ufficio: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Proroga contratto in scadenza

Adesione convenzioni CONSIP o del Soggetto Aggregatore di riferimento

Affidamento appalto di lavori, servizi e forniture di importo inferiore a 40.000 euro tramite il sistema dell'affidamento diretto

Affidamento appalto di servizi e forniture di importo superiore alle soglie di cui all'art. 35, D.Lgs. 50/2016 attraverso il sistema della procedura aperta

Affidamento appalto di servizi e forniture di importo pari o superiore a 40.000 euro e inferiore alle soglie di cui all'articolo 35, D.Lgs. 50/2016 mediante il sistema della procedura negoziata

Affidamento appalti di lavori di importo pari o superiore a 40.000 euro e inferiore a 200.000 euro mediante il sistema della procedura negoziata.

Affidamento appalti di lavori di importo pari o superiore a 40.000 euro e inferiore a 200.000 euro mediante il sistema della procedura negoziata, previa consultazione di almeno tre operatori economici.

Affidamento appalti di servizi e forniture di importo pari o superiore a 40.000 euro e inferiore alle soglie di cui all'art.35 D.Lgs.50/2016 attraverso il sistema della procedura negoziata previa consultazione di almeno 5 operatori economici.

Affidamento appalto di servizi e forniture di importo superiore alle soglie di cui all'art. 35 D. Lgs. 50/2016 s.m.i. attraverso il sistema della procedura aperta.

Affidamento appalti di lavori , servizi e forniture di importo inferiore a 40.000 euro tramite il sistema dell'affidamento diretto anche senza consultazione di due o piu' operatori economici.

Convenzioni con associazioni e altri enti di diritto privato non di competenza del Consiglio

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 51 -- Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato (Obbligo DPIA)
Settore	TUTTI I SETTORI - ATTIVITA' TRASVERSALE
Servizio	Tutti i Servizi - Attivita' trasversale
Ufficio: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accesso civico semplice concernente dati, documenti e informazioni soggetti a pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013

Accesso art. 22 e segg. della L. 241/90

Accesso civico generalizzato concernente dati e documenti ulteriori a quelli soggetti a pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 61 - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione
Settore	TUTTI I SETTORI - ATTIVITA' TRASVERSALE
Servizio	Tutti i Servizi - Attivita' trasversale
Ufficio: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	Maggioli SpA. P.I. 02066400405 Fisso: 0541 628111 Mail: maggiolispa@maggioli.it PEC: segreteria@maggioli.legalmail.it Maggioli S.p.A. P.Iva 02066400405 Fisso: 0541 628111 Mail: maggiolispa@maggioli.it PEC: segreteria@maggioli.legalmail.it
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete

	con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC

	4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative

	implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della

	vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure

	minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per

	favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate

	- MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Tenuta archivio corrente

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 69 - Trattamento effettuato tramite un sito web
Settore	TUTTI I SETTORI - ATTIVITA' TRASVERSALE
Servizio	Tutti i Servizi - Attivita' trasversale
Ufficio: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita

	l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del

	trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalità di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonché di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonché per documentare i provvedimenti adottati per porvi rimedio nonché per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione

	- MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Presentazione delle istanze in modalita' digitale attraverso un sito web

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 2 - Servizi alla Persona
Servizio	2.5 - Servizio Gare e Appalti
Ufficio: denominazione e punti di contatto	Ufficio Acquisti
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Acquisto arredi ed attrezzature di importo superiore alla soglia di Euro 5000.
Formazione e gestione Albo operatori economici.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 26 - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa
Settore	Settore 4 - Tecnico
Servizio	4.2 - Servizio Programmazione - Gestione LL.PP. - Manutenzioni - Demanio
Ufficio: denominazione e punti di contatto	Ufficio Ambiente e vigilanza ambientale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Interventi per il contrasto del randagismo

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 27 - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria
Settore	Settore 4 - Tecnico
Servizio	4.2 - Servizio Programmazione - Gestione LL.PP. - Manutenzioni - Demanio
Ufficio: denominazione e punti di contatto	Ufficio Ambiente e vigilanza ambientale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sospensione attivita'

Provvedimento per l'esecuzione d'ufficio in caso di mancata ottemperanza da parte dei destinatari a quanto precedentemente ordinato

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 4 - Tecnico
Servizio	4.2 - Servizio Programmazione - Gestione LL.PP. - Manutenzioni - Demanio
Ufficio: denominazione e punti di contatto	Ufficio Ambiente e vigilanza ambientale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamento rispetto limiti emissioni sonore per pubblici esercizi
Isole ecologiche: controllo servizio di raccolta

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale contrattualizzato presso il Comune (Obbligo DPIA)
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Amministrativo
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rilevazione presenze personale

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 19 - Trattamento di dati relativi ai trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.)
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Amministrativo
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio trattamenti sanitari obbligatori (T.S.O.) e di assistenza sanitaria obbligatoria (A.S.O.)

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 26 - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Amministrativo
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sequestri denaro o cose ai sensi del Reg. di P.U.

Commercio su aree pubbliche con posteggio in mercati - Controllo autorizzazioni

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Amministrativo
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Convenzione per adesione al servizio di consultazione Archivio Veicoli Rubati C.E.D. Interforze tramite i servizi telematici Ancitel

Convenzione per adesione all'utenza per il servizio di consultazione del C.E.D. della Direzione Generale della Motorizzazione Civile - Ministero delle Infrastrutture

Convenzione per la fornitura, mediante supporto informatico, di dati contenuti nel sistema informativo del Pubblico Registro Automobilistico

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 03 - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.3 - Servizi Demografici
Ufficio: denominazione e punti di contatto	Ufficio Anagrafe e Stato Civile
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e

	il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Anagrafe Comunicazioni Prefettura.
Anagrafe Comunicazioni all'ufficio tributi.
Anagrafe Tenuta registro unioni civili.
Stato Civile: Accettazione e tenuta dichiarazioni di testamento biologico.
Anagrafe certificati anagrafici.
Anagrafe: Variazioni anagrafiche AIRE (Anagrafe Italiani Residenti all'Esteri)
Anagrafe: Iscrizione AIRE (Anagrafe Italiani Residenti all'Esteri) dei cittadini italiani per trasferimento da AIRE o APR di altro Comune
Anagrafe: Ripristino immigrazione
Anagrafe: Verifica dichiarazione di rinnovo della dimora abituale
Anagrafe: Attestazione di regolarita' di soggiorno
Anagrafe: Attestazione di soggiorno permanente
Anagrafe rilascio carta di identita'
Anagrafe: Autentica di firma
Anagrafe: Autentica di copia
Anagrafe: Cancellazione anagrafiche AIRE (Anagrafe Italiani Residenti all'Esteri)
Anagrafe certificati anagrafici storici
Trasmissione dati: anagrafica e indirizzo popolazione per anno di nascita

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 04 - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile
Settore	Settore 3 - Economico e Finanziario
Servizio	3.3 - Servizi Demografici
Ufficio: denominazione e punti di contatto	Ufficio Anagrafe e Stato Civile
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamento requisiti di dimora abituale delle variazioni di residenza

Registro convivenze di fatto

Anagrafe iscrizioni registri anagrafici

Anagrafe cancellazione registri anagrafici per irreperibilita'.

Stato civile: Acquisizione della cittadinanza italiana per riconoscimento o dichiarazione giudiziale della filiazione durante la minore eta' del figlio, o nel caso in cui la paternita' o maternita' non puo' essere dichiarata, purché sia stato riconosciuto giudizialmente il diritto al mantenimento o agli alimenti, di minore straniero

Stato civile: Acquisizione della cittadinanza italiana per riconoscimento o dichiarazione giudiziale della filiazione o nel caso in cui la paternita' o maternita' non puo' essere dichiarata, purché sia stato riconosciuto giudizialmente il diritto al mantenimento o agli alimenti, di maggiorenne straniero

Anagrafe variazione di indirizzo.

Stato civile Tutela/Curatela.

Stato civile: Trascrizione atti di nascita formati all'estero

Stato civile Trasmissioni alla Procura della Repubblica.

Stato civile Comunicazioni all'Ufficio anagrafe.

Stato civile: Celebrazioni matrimoni civili

Stato civile: Pubblicazioni di matrimonio

Stato civile: Affiliazioni

Stato civile Disconoscimenti.

Stato civile Riconoscimenti.

Stato civile: Annotazione sentenza di rettificazione attribuzione di sesso

Stato civile: Annotazione sentenze di scioglimento del matrimonio civile, di cessazione degli effetti civili del matrimonio religioso (concordatario) o di delibazione sentenze ecclesiastiche di annullamento di matrimonio pronunciate in Italia, provenienti da altri comuni

Separazione consensuale, divorzio congiunto e modifica delle condizioni di separazione o di divorzio innanzi all'Ufficiale di Stato Civile

Stato Civile: Trascrizione atto di matrimonio celebrato all'estero

Stato civile: Adozione

Stato civile: Trascrizione atti di nascita rese dalla Direzione Sanitaria

Stato civile: Atto di nascita

Stato civile: Trascrizione atto di nascita neo-cittadino

Stato civile: Trascrizione atto di matrimonio celebrato in altro comune italiano

Stato Civile: Trascrizione atto di matrimonio concordatario

Stato civile: Redazione atto di morte

Stato civile: Trascrizione atto di morte avvenuta all'estero

Stato civile: Trascrizione atto di morte pervenuto da altro Comune

Stato Civile: Rilascio passaporto mortuario

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 05 - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo
Settore	Settore 3 - Economico e Finanziario
Servizio	3.3 - Servizi Demografici
Ufficio: denominazione e punti di contatto	Ufficio Anagrafe e Stato Civile
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Leva: Variazioni liste di leva
Leva Certificati di leva.
Leva: Variazioni liste di leva

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 07 - Trattamento di dati relativi all'attivita' di tenuta dell'elenco dei giudici popolari
Settore	Settore 3 - Economico e Finanziario
Servizio	3.3 - Servizi Demografici
Ufficio: denominazione e punti di contatto	Ufficio Anagrafe e Stato Civile
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Elettorale: aggiornamento Albo Giudici Popolari

Elettorale: iscrizione nell'albo dei Giudici Popolari

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.3 - Servizi Demografici
Ufficio: denominazione e punti di contatto	Ufficio Anagrafe e Stato Civile
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamento requisiti di dimora abituale delle variazioni di residenza

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 61 - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Archivio
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	Istituto per i Beni Artistici e Culturali dell'Emilia Romagna (IBACN) - ParER c.f. 80062590379 Tel. 051 527 6600 Pec: parer@postacert.regione.emilia-romagna.it. Plurima S.p.A. P.Iva 01698960547 Fisso: 075 605 96 69 Mail: plurima@plurima.info PEC: plurima@pec.plurimapec.com
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete

	con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC

	4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative

	implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della

	vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure

	minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per

	favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate

	- MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Archiviazione atti in archivio di deposito
Scarti di archivio
Tenuta archivio di deposito
Tenuta archivio storico

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 26 - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa
Settore	Settore 2 - Servizi alla Persona
Servizio	2.1 - Turismo, Manifestazioni e Promozione
Ufficio: denominazione e punti di contatto	Ufficio Artigianato
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e

	regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le

	prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle

	istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Segnalazione certificata di inizio attivita' (SCIA) attivita' artigianali in genere, compresi i laboratori di produzione, di trasformazione e/o confezionamento con/senza attivita' di vendita diretta al consumatore finale

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 37 - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Associazionismo e Volontariato
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Concessioni discrezionali non vincolate di contributi, benefici, esoneri e sovvenzioni (Provvedimenti amministrativi discrezionali nell'an e nel contenuto)

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 03 - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Autorizzazioni
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e

	il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rinvenimento oggetti smarriti

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 28 - Trattamento di dati relativi all'attivita' di rilascio di permessi per invalidi (Obbligo DPIA)
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Autorizzazioni
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rilascio contrassegno invalidi

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
Settore	Settore 1 - Affari Generali
Servizio	1.2 - Advocatura
Ufficio: denominazione e punti di contatto	Ufficio Advocatura
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Certificazione crediti

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 30 - Trattamento di dati relativi all'attivita' di consulenza giuridica, nonche' al patrocinio ed alla difesa in giudizio dell'amministrazione nonche' alla consulenza e copertura assicurativa in caso di responsabilita' civile verso terzi dell'amministrazione
Settore	Settore 1 - Affari Generali
Servizio	1.2 - Avvocatura
Ufficio: denominazione e punti di contatto	Ufficio Avvocatura
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controversie e contenziosi esterni ed interni, citazioni, costituzioni in giudizio, e conseguente nomina dei consulenti

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 49 - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento
Settore	Settore 1 - Affari Generali
Servizio	1.2 - Advocatura
Ufficio: denominazione e punti di contatto	Ufficio Advocatura
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la

	completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Lasciti

Convenzioni, transazioni ed ogni disposizione patrimoniale di straordinaria amministrazione

Autorizzazione al ricorso a transazioni e altri rimedi di risoluzione delle controversie alternativi a quelli giurisdizionali

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 1 - Affari Generali
Servizio	1.2 - Avvocatura
Ufficio: denominazione e punti di contatto	Ufficio Avvocatura
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Formazione Albo dei professionisti esterni.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 27 - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria
Settore	Settore 3 - Economico e Finanziario
Servizio	3.4 - Servizi Complementari
Ufficio: denominazione e punti di contatto	Ufficio Cimiteri
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio ai funerali - affidamento del servizio

Gestione e dislocamento delle salme

Sorveglianza sul collocamento delle ceneri in sepoltura o l'affidamento delle stesse ai familiari

Sospensione attivita'

Provvedimento per l'esecuzione d'ufficio in caso di mancata ottemperanza da parte dei destinatari a quanto precedentemente ordinato

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 26 - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa
Settore	Settore 2 - Servizi alla Persona
Servizio	2.1 - Turismo, Manifestazioni e Promozione
Ufficio: denominazione e punti di contatto	Ufficio Commercio
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalità di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e

	regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le

	prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle

	istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Modello - iniziativa di parte - SCIA commercio

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 46 - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche
Settore	Settore 4 - Tecnico
Servizio	4.1 - Servizio Urbanistica - Edilizia Privata - SUAP
Ufficio: denominazione e punti di contatto	Ufficio Condono Edilizio
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Condonò edilizio

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale contrattualizzato presso il Comune (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Contabilita' del personale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Liquidazione periodiche trattamenti accessori

Pensioni: Liquidazioni INPS - riscatti - ricongiunzioni

Rilascio certificato di stipendio/certificato di servizio

Stipendi e Paghe

Denuncia salari ed autoliquidazione INAIL

Certificazioni stipendio per cessione quinto - prestiti e cessioni

Rilevazione presenze personale

Certificazioni e modelli attestazioni relative alle posizioni giuridiche e posizioni assicurative (pa) dei dipendenti per uso ricongiunzioni riscatti e altro

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Contabilita' del personale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare,

	con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Liquidazione mensile indennità amministratori e periodiche dei consiglieri

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 43 - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Contabilita' del personale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare,

	con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Liquidazione del trattamento di fine mandato del Sindaco

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale contrattualizzato presso il Comune (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Contabilita' Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Ordinativi di incasso

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 37 - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Contabilita' Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Concessione tariffe agevolate

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Contabilita' Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Servizio di sorveglianza concessione in gestione impianti sportivi

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 38 - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.2 - Servizio Entrate e Tributi
Ufficio: denominazione e punti di contatto	Ufficio Contenzioso e mediazione tributaria
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controversie e contenziosi esterni ed interni, citazioni, costituzioni in giudizio, e conseguente nomina dei consulenti

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 2 - Servizi alla Persona
Servizio	2.5 - Servizio Gare e Appalti
Ufficio: denominazione e punti di contatto	Ufficio Contratti
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Consegna arredi e attrezzature uffici

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 60 - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio) (Obbligo DPIA)
Settore	Settore 2 - Servizi alla Persona
Servizio	2.5 - Servizio Gare e Appalti
Ufficio: denominazione e punti di contatto	Ufficio Contratti
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rogito atti segretario comunale
Autenticazione scritture private
Liquidazione diritti di segreteria
Registrazione contratti
Adempimenti conseguenti alla stipula del contratto
Pagamento delle spese di registrazione
Vidimazione repertorio
Adempimenti conseguenti alla stipula del contratto: registrazione anni successivi

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali
Settore	Segretario Generale
Servizio	Segretario Generale
Ufficio: denominazione e punti di contatto	Ufficio del Segretario Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare,

	con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo strategico ai sensi dell'art. 147-ter del D.Lgs. 267/2000

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 48 - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'
Settore	Segretario Generale
Servizio	Segretario Generale
Ufficio: denominazione e punti di contatto	Ufficio del Segretario Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Giornate della Trasparenza
Monitoraggio funzionamento PTPCT e monitoraggio singole misure
Tutela del dipendente che segnala illeciti e gestione delle segnalazioni.
Trasparenza e promozione trasparenza smart 2.0
Attivita' relativa alla gestione delle segnalazioni di illeciti
Attivazione del sistema di tutela del dipendente che segnala illeciti
Segnalazione-Esposto

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale contrattualizzato presso il Comune (Obbligo DPIA)
Settore	Settore 1 - Affari Generali
Servizio	1.0 Dirigente I Settore
Ufficio: denominazione e punti di contatto	Ufficio Dirigente I Settore
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Nomina Responsabile Unico del Procedimento (RUP)

Registro dei responsabili del trattamento relativo alle attività di trattamento dei dati personali

Registro del titolare del trattamento dei dati personali

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 36 - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti.
Settore	Settore 1 - Affari Generali
Servizio	1.0 Dirigente I Settore
Ufficio: denominazione e punti di contatto	Ufficio Dirigente I Settore
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli

	elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Ordinanze in qualita' di Ufficiale di governo

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 1 - Affari Generali
Servizio	1.0 Dirigente I Settore
Ufficio: denominazione e punti di contatto	Ufficio Dirigente I Settore
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati

	- MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo Green Pass lavoratori

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale contrattualizzato presso il Comune (Obbligo DPIA)
Settore	Settore 2 - Servizi alla Persona
Servizio	2.0 Dirigente II Settore
Ufficio: denominazione e punti di contatto	Ufficio Dirigente II Settore
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Nomina Responsabile Unico del Procedimento (RUP)

Registro dei responsabili del trattamento relativo alle attività di trattamento dei dati personali

Registro del titolare del trattamento dei dati personali

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 36 - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti.
Settore	Settore 2 - Servizi alla Persona
Servizio	2.0 Dirigente II Settore
Ufficio: denominazione e punti di contatto	Ufficio Dirigente II Settore
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli

	elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Ordinanze in qualita' di Ufficiale di governo

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 2 - Servizi alla Persona
Servizio	2.0 Dirigente II Settore
Ufficio: denominazione e punti di contatto	Ufficio Dirigente II Settore
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati

	- MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo Green Pass lavoratori

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale contrattualizzato presso il Comune (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.0 Dirigente III Settore
Ufficio: denominazione e punti di contatto	Ufficio Dirigente III Settore
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Nomina Responsabile Unico del Procedimento (RUP)

Registro dei responsabili del trattamento relativo alle attività di trattamento dei dati personali

Registro del titolare del trattamento dei dati personali

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 36 - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti.
Settore	Settore 3 - Economico e Finanziario
Servizio	3.0 Dirigente III Settore
Ufficio: denominazione e punti di contatto	Ufficio Dirigente III Settore
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli

	elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Ordinanze in qualita' di Ufficiale di governo

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.0 Dirigente III Settore
Ufficio: denominazione e punti di contatto	Ufficio Dirigente III Settore
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati

	- MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo Green Pass lavoratori

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale contrattualizzato presso il Comune (Obbligo DPIA)
Settore	Settore 4 - Tecnico
Servizio	4.0 Dirigente IV Settore
Ufficio: denominazione e punti di contatto	Ufficio Dirigente IV Settore
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Nomina Responsabile Unico del Procedimento (RUP)

Registro dei responsabili del trattamento relativo alle attività di trattamento dei dati personali

Registro del titolare del trattamento dei dati personali

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
Settore	Settore 4 - Tecnico
Servizio	4.0 Dirigente IV Settore
Ufficio: denominazione e punti di contatto	Ufficio Dirigente IV Settore
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Assistenza organi istituzionali: Gestione conferenze capigruppo.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 36 - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti.
Settore	Settore 4 - Tecnico
Servizio	4.0 Dirigente IV Settore
Ufficio: denominazione e punti di contatto	Ufficio Dirigente IV Settore
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli

	elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Ordinanze in qualita' di Ufficiale di governo

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 4 - Tecnico
Servizio	4.0 Dirigente IV Settore
Ufficio: denominazione e punti di contatto	Ufficio Dirigente IV Settore
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati

	- MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo Green Pass lavoratori

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Economato
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Fornitura cancelleria ed altro materiale di consumo per gli uffici

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 20 - Trattamenti relativi alla attivita' di concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario
Settore	Settore 4 - Tecnico
Servizio	4.1 - Servizio Urbanistica - Edilizia Privata - SUAP
Ufficio: denominazione e punti di contatto	Ufficio Edilizia Privata
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare,

	con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Certificazione idoneità alloggiativa.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 25 - Trattamento di dati relativi alla gestione delle procedure sanzionatorie
Settore	Settore 4 - Tecnico
Servizio	4.1 - Servizio Urbanistica - Edilizia Privata - SUAP
Ufficio: denominazione e punti di contatto	Ufficio Edilizia Privata
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sanzioni per interventi eseguiti in assenza o difformita' dalla segnalazione certificata di inizio attivita'

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
Settore	Settore 4 - Tecnico
Servizio	4.1 - Servizio Urbanistica - Edilizia Privata - SUAP
Ufficio: denominazione e punti di contatto	Ufficio Edilizia Privata
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Istituzioni di commissioni C.L.P.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 4 - Tecnico
Servizio	4.1 - Servizio Urbanistica - Edilizia Privata - SUAP
Ufficio: denominazione e punti di contatto	Ufficio Edilizia Privata
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Restituzione del contributo di costruzione/restituzione oneri

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo
Settore	Settore 3 - Economico e Finanziario
Servizio	3.4 - Servizi Complementari
Ufficio: denominazione e punti di contatto	Ufficio Elettorale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Elettorale: pubblicazione all'albo pretorio on-line dell'elenco dei cittadini che, pur essendo compresi nelle liste elettorali, non avranno compiuto, nel primo giorno fissato per le elezioni, il diciottesimo anno di eta'

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 05 - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo
Settore	Settore 3 - Economico e Finanziario
Servizio	3.4 - Servizi Complementari
Ufficio: denominazione e punti di contatto	Ufficio Elettorale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Elettorale Supporto commissioni elettorali.
Elettorale: autorizzazione al voto fuori sezione
Elettorale: voto domiciliare
Elettorale: voto assistito
Elettorale: rilascio tessera elettorale
Elettorale: revisione dinamica liste elettorali

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 06 - Trattamento di dati relativi all'attivita' di tenuta degli albi degli scrutatori e dei presidenti di seggio
Settore	Settore 3 - Economico e Finanziario
Servizio	3.4 - Servizi Complementari
Ufficio: denominazione e punti di contatto	Ufficio Elettorale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Elettorale iscrizione nell'albo degli scrutatori.

Elettorale: aggiornamento Albo scrutatori

Elettorale: aggiornamento Albo Presidenti di seggio

Elettorale: iscrizione nell'albo dei Presidenti di seggio

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 09 - Trattamento di dati relativi all'attivita' di tenuta delle liste di leva e dei registri matricolari
Settore	Settore 3 - Economico e Finanziario
Servizio	3.4 - Servizi Complementari
Ufficio: denominazione e punti di contatto	Ufficio Elettorale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Elettorale revisione semestrale liste elettorali.

Elettorale: revisione semestrale liste elettorali

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
Settore	Settore 3 - Economico e Finanziario
Servizio	3.4 - Servizi Complementari
Ufficio: denominazione e punti di contatto	Ufficio Elettorale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Istituzione commissioni permanenti, temporanee o speciali

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
Settore	Settore 2 - Servizi alla Persona
Servizio	2.5 - Servizio Gare e Appalti
Ufficio: denominazione e punti di contatto	Ufficio Forme Associative Intercomunali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Acquisizione di tutti gli atti e documenti necessari alla stipula dei contratti

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 2 - Servizi alla Persona
Servizio	2.5 - Servizio Gare e Appalti
Ufficio: denominazione e punti di contatto	Ufficio Gare e Appalti
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	Comune di Garlenda - C.F.: 00327980090 Borgata Ponte, n. 41 - 17033 Garlenda (SV)

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Maggioli Informatica - P.I. 02066400405
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Affidamento appalto di lavori di importo pari o superiore a 200.000 euro e inferiore a 1.000.000 di euro, mediante il sistema della procedura negoziata.

Affidamento appalti di lavori di importo pari o superiore a 200.000euro fino alle soglie di cui all'art. 35 del D.Lgs 50/2016 s.m.i. mediante il sistema della procedura aperta.

Affidamento appalto di lavori di importo pari o superiore a 1.000.000 di euro mediante il sistema della procedura aperta

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Gestione Giunta Comunale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Assistenza organi istituzionali: Gestione Giunta comunale.

Assistenza organi istituzionali Gestione Giunta comunale.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.2 - Servizio Entrate e Tributi
Ufficio: denominazione e punti di contatto	Ufficio ICI/IMU/TASI
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo ICI - IMU - TASI

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 29 - Trattamento di dati relativi al rilascio delle licenze e autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Igiene e Sanita'
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di

	climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei

	dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Autorizzazione a 1) apertura ed esercizio di una farmacia 2) trasferimento della farmacia dai locali gia' autorizzati ad altri situati nello stesso perimetro.

Assegnazione delle sedi farmaceutiche di nuova istituzione e delle sedi vacanti

Servizio di parafarmacia

Autorizzazione esercizio di somministrazione alimenti e bevande.

Autorizzazione esercizio preparazione alimenti e bevande.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Informatica
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Infocert SpA - P.Iva 07945211006 Tel. 06.54641489 Pec: infocert@legalmail.it Aruba SpA - P.Iva 01573850516 Tel. 0575 0500 Pec: aruba@aruba.pec.it Aruba pec SpA - P.Iva 01879020517 Tel. 0575 0500 Pec: arubapec@aruba.pec.it Telecom Italia S.p.A. - P.Iva 00488410010 Tel. 02 85951 Pec: telecomitalia@pec.telecomitalia.it - CESSATO - Soluzione S.r.l. P.Iva 02139650984 Tel. 030/2531939 Pec: soluzione@legalmail.it C & C Sistemi S.r.l. - P.Iva 00977740083 Fisso: 0183 290823 Mail: info@cecsistemi.it PEC: protocollo@pec.cecsistemi.it BM Soluzioni Ufficio S.r.l. - P.Iva 01322830090 Fisso: 0182 53025 Mail: posta@bmsoluzioni.it PEC: bmsoluzioni@pec.it Tekmeria S.r.l. - P.Iva P.Iva 01407510096 Fisso: 019 82 54 13 Mail: info@tekmeria.it Pec: tekmeriasrl@cg.legalmail.it Tecno World 2 S.r.l. P.Iva 03259940041 Fisso: 0182 73 30 891 Mail: amministrazione@tw2.eu Pec: tecnoworld2@pec.it ePublic S.r.l. P.Iva 01902060035 Fisso: 0321 39 73 95 0321-630228 Mail: info@epublic.it PEC: epublic@pcert.it - CESSATO - Espace Elab S.r.l.s. - P.Iva 01202580070 Cell.: 335 70 89 199 Tel. 0165 1840080 Mail: luca.ferrari@espaceelab.com Pec: elabsas@pec.uno.it
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - APPARECCHIATURE-ICT: attacchi informatici/azione di virus/codici maligni - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei

	software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI

	AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE

	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA INCIDENTI: crimeware (malware che mirano a ottenere il controllo dei sistemi) - CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - TRATTAMENTI ELETTRONICI: utilizzo di parole chiave non adeguate - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla	Alto

prospettiva degli interessati	

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni

	rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalità di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarità impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - Tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003 - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuità dell'alimentazione elettrica

Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalità di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonché di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti

Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Gestione sito web: gestione in hosting
AGID Acquisto e consegna firma digitali.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 59 - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Informatica
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	Infocert SpA - P.Iva 07945211006 Tel. 06.54641489 Pec: infocert@legalmail.it Aruba SpA - P.Iva 01573850516 Tel. 0575 0500 Pec: aruba@aruba.pec.it Aruba pec SpA - P.Iva 01879020517 Tel. 0575 0500 Pec: arubapec@aruba.pec.it Telecom Italia S.p.A. - P.Iva 00488410010 Tel. 02 85951 Pec: telecomitalia@pec.telecomitalia.it - CESSATO - Soluzione S.r.l. P.Iva 02139650984 Tel. 030/2531939 Pec: soluzione@legalmail.it C & C Sistemi S.r.l. - P.Iva 00977740083 Fisso: 0183 290823 Mail: info@cecsistemi.it PEC: protocollo@pec.cecsistemi.it BM Soluzioni Ufficio S.r.l. - P.Iva 01322830090 Fisso: 0182 53025 Mail: posta@bmsoluzioni.it PEC: bmsoluzioni@pec.it Tekmeria S.r.l. - P.Iva P.Iva 01407510096 Fisso: 019 82 54 13 Mail: info@tekmeria.it Pec: tekmeriasrl@cg.legalmail.it Tecno World 2 S.r.l. P.Iva 03259940041 Fisso: 0182 73 30 891 Mail: amministrazione@tw2.eu Pec: tecnoworld2@pec.it ePublic S.r.l. P.Iva 01902060035 Fisso: 0321 39 73 95 0321-630228 Mail: info@epublic.it PEC: epublic@pcert.it - CESSATO - Espace Elab S.r.l.s. - P.Iva 01202580070 Cell.: 335 70 89 199 Tel. 0165 1840080 Mail: luca.ferrari@espaceelab.com Pec: elabsas@pec.uno.it
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione

	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di

	intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione

	dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI

Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal

	disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalità di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarità impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuità dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorità del titolare e del responsabile del trattamento, e divieto di trattamento dei dati

	personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalità di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonché di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonché per documentare i provvedimenti adottati per porvi rimedio nonché per gestire le

	violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sicurezza dei processi - servizi informatici

Sviluppo software: Installazione/configurazione nuovo software applicativo

Sviluppo software: Acquisizione servizio di manutenzione

Gestione S.I. e rete: Acquisizione fornitura connettivita'

Gestione S.I. e rete: Configurazione connettivita'

Gestione S.I. e rete: Backup dei dati

Gestione S.I. e rete: Aggiornamento backup

Gestione S.I. e rete: Configurazione utenti di rete

Gestione S.I. e rete: Configurazione apparati di rete

Gestione S.I. e rete: Creazione caselle di posta elettronica

Gestione S.I. e rete: Aggiornamenti automatici sw di base e produttivita'

Gestione S.I. e rete: Aggiornamento antivirus

Gestione S.I. e rete: Installazione stampanti di rete

Gestione S.I. e rete: Gestione server di rete

Gestione S.I. e rete: Gestione delle password.

Gestione S.I. e rete: Manuale sicurezza informatica

Assistenza utenti: Interventi di consulenza/addestramento

Assistenza utenti: Interventi manutenzione hardware/software

Assistenza utenti: Invio denunce all'agenzia dell'entrate via ENTRATEL

Assistenza utenti: Gestione banche dati esterne

Assistenza utenti: Interventi supporto per la gestione dati applicativi

Assistenza utenti: INA SAIA

Gestione tecnologica SIT: Creazione banca dati geografica

Gestione tecnologica SIT: Interventi per la normalizzazione delle banche dati

Gestione tecnologica SIT: Formazione GIS

Gestione S.I. e rete: Analisi dei fabbisogni, programmazione e gestione della rete informatica

AGID: Dematerializzazione dei documenti

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Valutazione di impatto sulla protezione dei dati (DPIA) conforme alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD singola valutazione che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 68 - Trattamento dei dati personali ottenuti tramite riprese audio-video durante le sedute del consiglio comunale.
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Informatica
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Edinet Srl - P. IVA 01438900092 corso Italia n. 66 - Pietra Ligure Infocert SpA - P.Iva 07945211006 Tel. 06.54641489 Pec: infocert@legalmail.it Aruba pec SpA - P.Iva 01879020517 Tel. 0575 0500 Pec: arubapec@aruba.pec.it Aruba SpA - P.Iva 01573850516 Tel. 0575 0500 Pec: aruba@aruba.pec.it Telecom Italia S.p.A. - P.Iva 00488410010 Tel. 02 85951 Pec: telecomitalia@pec.telecomitalia.it - CESSATO - Soluzione S.r.l. P.Iva 02139650984 Tel. 030/2531939 Pec: soluzione@legalmail.it - CESSATO - Espace Elab S.r.l.s. - P.Iva 01202580070 Cell.: 335 70 89 199 Tel. 0165 1840080 Mail: luca.ferrari@espaceelab.com Pec: elabsas@pec.uno.it ePublic S.r.l. P.Iva 01902060035 Fisso: 0321 39 73 95 0321-630228 Mail: info@epublic.it PEC: epublic@pcert.it Tecno World 2 S.r.l. P.Iva 03259940041 Fisso: 0182 73 30 891 Mail: amministrazione@tw2.eu Pec: tecnoworld2@pec.it Tekmeria S.r.l. - P.Iva P.Iva 01407510096 Fisso: 019 82 54 13 Mail: info@tekmeria.it Pec: tekmeriasrl@cg.legalmail.it BM Soluzioni Ufficio S.r.l. - P.Iva 01322830090 Fisso: 0182 53025 Mail: posta@bmsoluzioni.it PEC: bmsoluzioni@pec.it Maggioli S.p.A. P.Iva 02066400405 Fisso: 0541 628111 Mail: maggiolispa@maggioli.it PEC: segreteria@maggioli.legalmail.it C & C Sistemi S.r.l. - P.Iva 00977740083 Fisso: 0183 290823 Mail: info@cecsistemi.it PEC: protocollo@pec.cecsistemi.it
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- OPERATORI: errore umano nella gestione del trattamento - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2):

	INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed

	eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-11 - PRESCRIZIONI: nell'attivita' di videosorveglianza prescrizione del rispetto di tutte le misure e gli accorgimenti prescritti Autorita' Garante come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpelllo - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante

	- MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI**

ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Riprese e registrazione audio e video delle sedute del Consiglio Comunale

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Informazioni
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamento requisiti di dimora abituale delle variazioni di residenza
Controllo - Ispezione

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 24 -Trattamento di dati relativi all'infortunistica stradale
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Infortunistica
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rilievo incidente

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Infortunistica
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sequestro di veicoli coinvolti nel sinistro

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 4 - Tecnico
Servizio	4.2 - Servizio Programmazione - Gestione LL.PP. - Manutenzioni - Demanio
Ufficio: denominazione e punti di contatto	Ufficio Lavori Pubblici
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Varianti in corso d'opera lavori in appalto

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 4 - Tecnico
Servizio	4.2 - Servizio Programmazione - Gestione LL.PP. - Manutenzioni - Demanio
Ufficio: denominazione e punti di contatto	Ufficio Lavori Pubblici
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Liquidazioni acconti o rata di saldo e omologa del certificato di regolare esecuzione per contratti pubblici di lavori, servizi e forniture in economia
Coordinatore della sicurezza in fase di progettazione
Affidamento direzione lavori in appalto a professionisti esterni
Alta sorveglianza lavori eseguiti in project financing o in convenzione con altri soggetti terzi
Partecipazione a commissioni di collaudo
Affidamento incarico esterno di coordinatore della sicurezza
Progettazione esterna (preliminare, definitiva, esecutiva)
Direzione lavori
Collaudo
Subappalto
Redazione cronoprogramma
Affidamento appalto di lavori di importo pari o superiore a 1.000.000 di euro mediante il sistema della procedura aperta
Concessioni canali demaniali irrigui

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale contrattualizzato presso il Comune (Obbligo DPIA)
Settore	Settore 4 - Tecnico
Servizio	4.2 - Servizio Programmazione - Gestione LL.PP. - Manutenzioni - Demanio
Ufficio: denominazione e punti di contatto	Ufficio Manutenzione Edifici - Impianti - Infrastrutture
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Pronta reperibilità

Rilevazione presenze personale

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 4 - Tecnico
Servizio	4.2 - Servizio Programmazione - Gestione LL.PP. - Manutenzioni - Demanio
Ufficio: denominazione e punti di contatto	Ufficio Manutenzione Edifici - Impianti - Infrastrutture
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sopralluogo

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 57 - Trattamento di dati relativi all'attivita' di tenuta dell'albo e delle notifiche dell'Ente e di altre pubbliche amministrazioni
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Messi
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Albo e notifiche
Pubblicazioni albo on line.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 20 - Trattamenti relativi alla attivita' di concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario
Settore	Settore 4 - Tecnico
Servizio	4.2 - Servizio Programmazione - Gestione LL.PP. - Manutenzioni - Demanio
Ufficio: denominazione e punti di contatto	Ufficio Patrimonio immobiliare
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare,

	con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Assegnazione di aree per l'edilizia residenziale pubblica

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 4 - Tecnico
Servizio	4.2 - Servizio Programmazione - Gestione LL.PP. - Manutenzioni - Demanio
Ufficio: denominazione e punti di contatto	Ufficio Patrimonio immobiliare
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - APPARECCHIATURE-ICT: attacchi informatici/azione di virus/codici maligni - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle

	specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure

	minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA INCIDENTI: crimeware (malware che mirano a ottenere il controllo dei sistemi) - CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento -TRATTAMENTI ELETTRONICI: utilizzo di parole chiave non adeguate - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e

	relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non

	autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - Tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003 - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del

	trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Locazione immobili urbani

Vendita beni patrimonio disponibile mediante asta pubblica

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale contrattualizzato presso il Comune (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Personale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

L.104-Anagrafe prestazioni - gestione scioperi - gestione permessi sindacali.
Assunzione di personale mediante concorsi, mobilità e contratti di lavoro a tempo determinato o flessibile
Selezioni da centro per l'impiego
Stabilizzazioni
Mobilità dall'esterno ex art. 30 del D.Lgs. 165/2001
Mobilità ex art. 34 bis, D.Lgs. 165/2001
Mobilità interna intersettoriale da P.E.G.
Cambi di profilo professionale
Trasformazione del rapporto di lavoro a tempo parziale
Denunce infortuni sul lavoro
Procedimento disciplinare
Comandi e trasferimenti
Autorizzazioni a prestazioni professionali di personale interno a tempo indeterminato e determinato -
Autorizzazione ai dipendenti allo svolgimento di incarichi non compresi nei compiti e doveri d'ufficio a favore di terzi
Nomina componenti del CUG
Rilevazione eccedenze personale
Attribuzione incarichi dirigenziali
Certificazioni e modelli attestazioni relative alle posizioni giuridiche e posizioni assicurative (pa) dei dipendenti per uso ricongiunzioni riscatti e altro
Attribuzione progressioni economiche orizzontali o di carriera
Attribuzione e revoca incarichi al personale dirigente
Costituzione di ufficio posto alle dirette dipendenze del sindaco ai sensi dell'art. 90, TUEL

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Personale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Attività sindacale di nomina, attribuzione e revoca incarichi.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 02 -Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Personale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it

Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete

	con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC

	4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative

	implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della

	vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure

	minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per

	favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate

	- MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonché da riconoscimento di inabilita' a svolgere attivita' lavorativa

Denuncia annuale rilevazione disabili

Assunzione personale appartenente a categorie protette (Legge 68/1999)

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Personale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita

	l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-11 - PROTEZIONE AREE E LOCALI: custodia in armadi blindati e/o ignifughi - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili - MS-LOG-14 - PROTEZIONE AREE E LOCALI: custodia dei supporti

	in contenitori sigillati - MS-LOG-15 - PROTEZIONE AREE E LOCALI: verifica della leggibilita' dei supporti
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-11 - PRESCRIZIONI: nell'attivita' di videosorveglianza prescrizione del rispetto di tutte le misure e gli accorgimenti prescritti Autorita' Garante come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpelllo - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari

	- MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonché di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee guida di sicurezza - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-22 - SISTEMA GESTIONE PRIVACY: registrazione delle consultazioni - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici - MS-ORG-25 - SISTEMA GESTIONE PRIVACY: verifiche periodiche su dati o trattamenti non consentiti o non corretti - MS-ORG-23 - SISTEMA GESTIONE PRIVACY: distruzione controllata dei supporti - MS-ORG-24 - SISTEMA GESTIONE PRIVACY: piano di disaster recovery
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonché per documentare i provvedimenti adottati per porvi rimedio nonché per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalità di scambio dei dati

	personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Il trattamento dei dati personali e' finalizzato esclusivamente alla verifica, da parte del Titolare o suoi delegati, del possesso delle certificazioni verdi digitali COVID-19:

- Green Pass base in corso di validita',
per consentire l'accesso agli uffici e ai locali dell'ente. Il controllo del Green pass base, per l'accesso agli uffici e locali dell'ente ha per oggetto:
 - l'intervenuta vaccinazione;
 - il risultato negativo a un test molecolare nelle ultime 72 ore o antigenico rapido nelle 48 ore precedenti;
 - la guarigione da covid-19 da non piu' di sei mesi.
- Per accedere invece alla biblioteca comunale, il controllo ha per oggetto:
- Green Pass rafforzato a partire dai 12 anni compiuti

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 43 - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Personale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare,

	con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Versamenti contributivi datori di lavoro

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 39 - Trattamento di dati relativi alle attivita' ricreative, di promozione dei giovani.
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Politiche Giovanili
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - APPARECCHIATURE-ICT: attacchi informatici/azione di virus/codici maligni - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA INCIDENTI: crimeware (malware che mirano a ottenere il controllo dei sistemi) - CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - TRATTAMENTI ELETTRONICI: utilizzo di parole chiave non adeguate - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e

	relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non

	autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - Tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003 - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del

	trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non

	espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Albo contributi - Manifestazioni - Corsi

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 11- Trattamento di dati relativi all'attivita' di assistenza scolastica ai portatori di handicap o con disagio psico-sociale
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Politiche Scolastiche ed educative
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	Istituto Comprensivo Alassio - C.F. 90051580091 Via Gerolamo Gastaldi, 32 - 17021 Alassio (SV) - https://www.istitutocomprensivoalassio.edu.it/ Scuola Elementare Statale Via Negrelli 5 - 17021 Alassio (SV) - 0182

contatto	643909
Responsabile trattamento: denominazione e punti di contatto	Istituto Salesiano "Madonna degli Angeli" - PI 00328100094 Via San Giovanni Bosco, 12 17021 Alassio CROCE ROSSA - C.F. 90059480096 CROCE BIANCA - C.F. 81001010099 TPL Linea Srl - Savona - PI: IT01556040093 Via Valletta S. Cristoforo, 3R 17100 Savona
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI

	PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e

	relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non

	autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi

	degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal

	disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio di assistenza educativa alunni disabili in ambito scolastico

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 14 - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Politiche Scolastiche ed educative
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Istituto Salesiano "Madonna degli Angeli" - PI 00328100094 Via San Giovanni Bosco, 12 17021 Alassio CROCE ROSSA - C.F. 90059480096 CROCE BIANCA - C.F. 81001010099 TPL Linea Srl - Savona - PI: IT01556040093 Via Valletta S. Cristoforo, 3R 17100 Savona
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza

	ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con

	violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed

	eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e

	restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio di fornitura testi scolastici per alunni della scuola primaria

Servizio di gestione tariffe e rette

Concessione prestazioni agevolate (servizi educativi, socio-assistenziali, etc.)

Servizio di controllo I.S.E.E. per prestazioni sociali agevolate

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 21 - Trattamento di dati relativi alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Politiche Scolastiche ed educative
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	Istituto Comprensivo Alassio - C.F. 90051580091 Via Gerolamo Gastaldi, 32 - 17021 Alassio (SV) - https://www.istitutocomprensivoalassio.edu.it/ Scuola Elementare Statale Via Negrelli 5 - 17021 Alassio (SV) - 0182

contatto	643909
Responsabile trattamento: denominazione e punti di contatto	Istituto Salesiano "Madonna degli Angeli" - PI 00328100094 Via San Giovanni Bosco, 12 17021 Alassio CROCE ROSSA - C.F. 90059480096 CROCE BIANCA - C.F. 81001010099 TPL Linea Srl - Savona - PI: IT01556040093 Via Valletta S. Cristoforo, 3R 17100 Savona
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI

	PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e

	relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non

	autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi

	degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal

	disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Collocazione fasce tariffarie I.S.E.E. servizi scolastici ed educativi.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 22 - Trattamento di dati relativi all'attivita' di formazione ed in favore del diritto allo studio .
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Politiche Scolastiche ed educative
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	Istituto Comprensivo Alassio - C.F. 90051580091 Via Gerolamo Gastaldi, 32 - 17021 Alassio (SV) - https://www.istitutocomprensivoalassio.edu.it/ Scuola Elementare Statale Via Negrelli 5 - 17021 Alassio (SV) - 0182

contatto	643909
Responsabile trattamento: denominazione e punti di contatto	Istituto Salesiano "Madonna degli Angeli" - PI 00328100094 Via San Giovanni Bosco, 12 17021 Alassio CROCE ROSSA - C.F. 90059480096 CROCE BIANCA - C.F. 81001010099 TPL Linea Srl - Savona - PI: IT01556040093 Via Valletta S. Cristoforo, 3R 17100 Savona
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI

	PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e

	relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non

	autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi

	degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal

	disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio centro ricreativo estivo - CRE

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 37 - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Politiche Scolastiche ed educative
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	Istituto Comprensivo Alassio - C.F. 90051580091 Via Gerolamo Gastaldi, 32 - 17021 Alassio (SV) - https://www.istitutocomprensivoalassio.edu.it/

trattamento: denominazione e punti di contatto	Scuola Elementare Statale Via Negrelli 5 - 17021 Alassio (SV) - 0182 643909
Responsabile trattamento: denominazione e punti di contatto	Istituto Salesiano "Madonna degli Angeli" - PI 00328100094 Via San Giovanni Bosco, 12 17021 Alassio CROCE ROSSA - C.F. 90059480096 CROCE BIANCA - C.F. 81001010099 TPL Linea Srl - Savona - PI: IT01556040093 Via Valletta S. Cristoforo, 3R 17100 Savona
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza

	ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con

	violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed

	eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e

	restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Concessione contributo a istituti scolastici paritari

Concessione contributo regionale buono-libri

Concessioni discrezionali non vincolate di contributi, benefici, esoneri e sovvenzioni (Provvedimenti amministrativi discrezionali nell'an e nel contenuto)

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Politiche Scolastiche ed educative
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Istituto Salesiano "Madonna degli Angeli" - PI 00328100094 Via San Giovanni Bosco, 12 17021 Alassio CROCE ROSSA - C.F. 90059480096 CROCE BIANCA - C.F. 81001010099 TPL Linea Srl - Savona - PI: IT01556040093 Via Valletta S. Cristoforo, 3R 17100 Savona
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza

	ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con

	violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed

	eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e

	restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio accreditamenti servizi socio-assistenziali

Procedura per l'affidamento del servizio pre post scuola e prolungamento scolastico.

Servizio di ristorazione scolastica

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 10 - Trattamento di dati relativi alla attivita' di assistenza domiciliare
Settore	Settore 2 - Servizi alla Persona
Servizio	2.3 - Servizio Politiche Sociali
Ufficio: denominazione e punti di contatto	Ufficio Politiche Sociali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	Ambito Territoriale Sociale 16

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio di assistenza domiciliare (pasti, lavanderia, ore di assistenza, accompagnamenti ect...)
Sostegno educativo alunni disabili domiciliare e scolastica.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 11- Trattamento di dati relativi all'attivita' di assistenza scolastica ai portatori di handicap o con disagio psico-sociale
Settore	Settore 2 - Servizi alla Persona
Servizio	2.3 - Servizio Politiche Sociali
Ufficio: denominazione e punti di contatto	Ufficio Politiche Sociali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sostegno educativo alunni disabili in ambito scolastico.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 12 - Trattamento di dati relativi alla attivita' di gestione delle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc
Settore	Settore 2 - Servizi alla Persona
Servizio	2.3 - Servizio Politiche Sociali
Ufficio: denominazione e punti di contatto	Ufficio Politiche Sociali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	Ambito Territoriale Sociale 16

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le

	procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli

	elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Inserimenti in strutture es.RSA, RP,CD

Controlli esistenza in vita per misure gravissime disabilita'.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 13 - Trattamento di dati relativi all'attivita' ricreative per la promozione del benessere della persona e della comunita', per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale
Settore	Settore 2 - Servizi alla Persona
Servizio	2.3 - Servizio Politiche Sociali
Ufficio: denominazione e punti di contatto	Ufficio Politiche Sociali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	Ambito Territoriale Sociale 16

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Attivita' motoria -Centro Anziani -con GE.S.CO.
Centro sociale per anziani Isola che c'e'
Servizio di segretariato sociale
Accessi sportello di cittadinanza.
progetto con Cooperativa sociale SOS pratiche.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 14 - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)
Settore	Settore 2 - Servizi alla Persona
Servizio	2.3 - Servizio Politiche Sociali
Ufficio: denominazione e punti di contatto	Ufficio Politiche Sociali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	Ambito Territoriale Sociale 16

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Concessione integrazione rette case di riposo
Concessione contributi economici
Reddito di inclusione.
Servizio di controllo I.S.E.E. per prestazioni sociali agevolate
Prestazioni agevolate - (rette) nido e assistenza domiciliare.
Bonus gas/energia/idrico.
assegno maternita' -assegno nucleo numeroso.
Reddito di cittadinanza.
Inserimento in percorsi di inclusione sociale.
Misure regionali/distrettuali: fondo non autosufficienza -MAC (Meglio a casa) vita indigente - custodi sociali.
Gestione delle emergenze sanitarie e delle misure sanitarie, socio-assistenziali, economiche, fiscali, di prevenzione e di sostegno previste dalla legge, dai regolamenti e/o imposte dalle Autorita' competenti a gestire l'emergenza

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 18 - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori
Settore	Settore 2 - Servizi alla Persona
Servizio	2.3 - Servizio Politiche Sociali
Ufficio: denominazione e punti di contatto	Ufficio Politiche Sociali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	Ambito Territoriale Sociale 16

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e

	il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Procedure correlate alla nomina amministratore di sostegno, interdizione o inabilitazione.

Minori in affido ed adozione.

Inserimento minori affidati in comunita' o famiglie affidatarie.

Minori rapporti con Tribunale dei minorenni e Tribunale Ordinario.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 19 - Trattamento di dati relativi ai trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.)
Settore	Settore 2 - Servizi alla Persona
Servizio	2.3 - Servizio Politiche Sociali
Ufficio: denominazione e punti di contatto	Ufficio Politiche Sociali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	Ambito Territoriale Sociale 16

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio trattamenti sanitari obbligatori (T.S.O.) e di assistenza sanitaria obbligatoria (A.S.O.)

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 20 - Trattamenti relativi alla attivita' di concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario
Settore	Settore 2 - Servizi alla Persona
Servizio	2.3 - Servizio Politiche Sociali
Ufficio: denominazione e punti di contatto	Ufficio Politiche Sociali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	Ambito Territoriale Sociale 16

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare,

	con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

alloggi ERP (morosita',decadenza, graduatorie ecc...)

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 21 - Trattamento di dati relativi alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie
Settore	Settore 2 - Servizi alla Persona
Servizio	2.3 - Servizio Politiche Sociali
Ufficio: denominazione e punti di contatto	Ufficio Politiche Sociali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	Ambito Territoriale Sociale 16

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Iscrizioni e graduatorie per erogazione servizio
Controlli vaccinali per nido d'infanzia.
Voucher nidi.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 37 - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati
Settore	Settore 2 - Servizi alla Persona
Servizio	2.3 - Servizio Politiche Sociali
Ufficio: denominazione e punti di contatto	Ufficio Politiche Sociali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	Ambito Territoriale Sociale 16

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Concessioni discrezionali non vincolate di contributi, benefici, esoneri e sovvenzioni a associazioni/enti.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 27 - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria
Settore	Settore 2 - Servizi alla Persona
Servizio	2.1 - Turismo, Manifestazioni e Promozione
Ufficio: denominazione e punti di contatto	Ufficio Polizia Amministrativa
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sospensione attivita'

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 26 - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Polizia Giudiziaria
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA

	(PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Trasmissione notizie di reato all'A.G.
Indagini su delega Procura

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 27 - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Polizia Giudiziaria
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA

	(PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamento di conformita' per la sanatoria degli abusi edilizi

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale contrattualizzato presso il Comune (Obbligo DPIA)
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Protezione Civile (sezione amministrativa)
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Esercitazione e formazione del personale interno

Partecipazione a coordinamenti intercomunali

Vigilanza sanitaria a cura del medico competente limitatamente al personale impegnato nel servizio di Protezione Civile.

Gestione di Lavoratori di Pubblica Utilità che prestano lavoro non retribuito a favore della Comunità presso il Comune o enti ed organizzazioni di volontariato.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 36 - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti.
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Protezione Civile (sezione amministrativa)
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli

	elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Censimento dei danni e individuazione degli interventi necessari per il superamento dell'emergenza

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 40 - Trattamento di dati relativi alla tenuta albi comunali Associazioni e Organizzazioni di Volontariato nonche' all'attivita' di relativa agli organismi di decentramento e di partecipazione (Obbligo DPIA)
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Protezione Civile (sezione amministrativa)
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le

	modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Aggiornamento dell'Elenco delle Associazioni incluse nelle attivita' di protezione civile

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Protezione Civile (sezione amministrativa)
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Convenzioni con associazioni di volontariato

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 36 - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti.
Settore	Settore 4 - Tecnico
Servizio	4.2 - Servizio Programmazione - Gestione LL.PP. - Manutenzioni - Demanio
Ufficio: denominazione e punti di contatto	Ufficio Protezione Civile (sezione tecnica)
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli

	elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Censimento dei danni e individuazione degli interventi necessari per il superamento dell'emergenza
Interventi di somma urgenza

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Protocollo
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizi postali

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 61 - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Protocollo
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gestione e acquisizione degli atti e della posta in arrivo e in partenza per la registrazione sul protocollo informatico

Stampa giornaliera ed annuale del registro di protocollo informatico

Annullamenti di protocollo per errata assegnazione

Accettazione, protocollazione e smistamento delle partecipazioni a gare

Protezione dei dati personali

Aggiornamento manuale di gestione

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Rapporti con le Societa' Partecipate
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	GE.S.CO. srl indirizzo: via A. Canata, 7 - 17021 Alassio Fisso: 0182 642846 Fax: 0182 649763

contatto	Sito web istituzionale http://www.gescoalassio.it/
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare,

	con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Attività sindacale di nomina, attribuzione e revoca incarichi.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Rapporti con le Societa' Partecipate
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	GE.S.CO. srl indirizzo: via A. Canata, 7 - 17021 Alassio Fisso: 0182 642846 Fax: 0182 649763

denominazione e punti di contatto	Sito web istituzionale http://www.gescoalassio.it/
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Designazione e revoca dei rappresentanti del Comune presso enti, aziende e istituzioni

Nomine e affidamenti incarichi per prestazioni o servizi per i quali le determinazioni siano fondate su rapporti fiduciari

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 26 - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Segnaletica
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Ordinanze regolamentazione circolazione

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale contrattualizzato presso il Comune (Obbligo DPIA)
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Segreteria Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Nomina e revoca assessori

Nomina Segretario generale

Nomina Organismo di valutazione

Costituzione di ufficio posto alle dirette dipendenze del sindaco ai sensi dell'art. 90, TUEL

Attribuzione e revoca incarichi al personale dirigente

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Segreteria Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Attività di segreteria nucleo di valutazione

Attività sindacale di nomina, attribuzione e revoca incarichi.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Segreteria Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalità di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non

	autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati

	personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalità di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonché di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonché per documentare i provvedimenti adottati per porvi rimedio nonché per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di

	autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Agenda Sindaco ed Assessori

Assistenza organi istituzionali: Gestione commissioni consiliari.

Assistenza organi istituzionali: Gestione conferenze capigruppo.

Comune di Alassio
Piazza Liberta' 3
17021 Alassio SV

Assistenza organi istituzionali: Gestione Consiglio comunale.
Assistenza organi istituzionali: Approvazione verbali consiglio
Assistenza organi istituzionali: Nomina Presidente e vicepresidenti
Assistenza organi istituzionali: Decadenze
Designazione e revoca dei rappresentanti del Comune presso enti, aziende e istituzioni
Liquidazione mensile indennita' amministratori e periodiche dei consiglieri
Nomine e affidamenti incarichi per prestazioni o servizi per i quali le determinazioni siano fondate su rapporti fiduciari
Assistenza organi istituzionali: Convalida consiglieri
Anagrafe degli eletti: Pubblicazione e aggiornamento dati on line

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Segreteria Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare,

	con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Redazione delibera/determina

Consulenza e assistenza del Segretario/Direttore agli organi di indirizzo politico

Mozioni, ordini del giorno, risoluzioni, interrogazioni ed interpellanze

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 37 - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Segreteria Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Registro delle onoreficenze.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Segreteria Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo successivo di regolarita' amministrativa e contabile ai sensi dell'art. 147-bis del D.Lgs. 267/2000

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 51 -- Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato (Obbligo DPIA)
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Segreteria Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accesso art. 43, co. 2 del T.U.E.L. da parte dei consiglieri
Registro degli accessi

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 60 - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio) (Obbligo DPIA)
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Segreteria Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Adempimenti conseguenti alla stipula del contratto

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 61 - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Segreteria Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Archiviazione deliberazioni/determinazioni

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Valutazione di impatto sulla protezione dei dati (DPIA) conforme alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD singola valutazione che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 68 - Trattamento dei dati personali ottenuti tramite riprese audio-video durante le sedute del consiglio comunale.
Settore	Settore 1 - Affari Generali
Servizio	1.1 - Servizio Attivita' informative
Ufficio: denominazione e punti di contatto	Ufficio Segreteria Generale
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- OPERATORI: errore umano nella gestione del trattamento - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli	Alto

interessati	

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarità impianti - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuità dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative - MS-ORG-11 - PRESCRIZIONI: nell'attività di videosorveglianza prescrizione del rispetto di tutte le misure e gli accorgimenti prescritti Autorità Garante come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorità del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati

	membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA

	(PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Assistenza organi istituzionali: Trascrizione verbali consiglio

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
Settore	Settore 3 - Economico e Finanziario
Servizio	3.1 - Servizio Programmazione, Contabilita' e Controllo di Gestione
Ufficio: denominazione e punti di contatto	Ufficio Sorveglianza Sanitaria (Sosa)
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Medico competente - nomina

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 29 - Trattamento di dati relativi al rilascio delle licenze e autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Sport
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di

	climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei

	dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Pubblica sicurezza palestre - Autorizzazione

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 37 - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Sport
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Concessione di premi in occasione di manifestazioni sportive
Concessione contributi straordinari a concessionari di impianti
Concessione contributi per manifestazioni
Concessione contributi ad associazioni sportive dilettantistiche
Concessione tariffe agevolate
Concessione contributi ordinari in denaro a sostegno dell'attivita' ordinaria del privato, dell'ente o dell'associazione richiedente

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 39 - Trattamento di dati relativi alle attivita' ricreative, di promozione dei giovani.
Settore	Settore 2 - Servizi alla Persona
Servizio	2.4 - Servizio Politiche Scolastiche, Sport, Igiene e Sanita'
Ufficio: denominazione e punti di contatto	Ufficio Sport
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio fornitura corsi promozionali di attività sportiva
Servizio di promozione attività di educazione sportiva scuole
Autorizzazione per eventi e manifestazioni negli impianti sportivi

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 41 - Trattamento di dati per scopi statistici effettuati da SISTAN (Ufficio Comunale di statistica)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.3 - Servizi Demografici
Ufficio: denominazione e punti di contatto	Ufficio Statistica
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Implicazioni derivanti dalla previsione di cui all'art. 3, comma 1, del d.lgs. n. 33/2013, in base alla quale i dati e i documenti forniti al richiedente tramite l'accesso generalizzato sono considerati come "pubblici" - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati

	- MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-11 - PRESCRIZIONI: nell'attivita' di videosorveglianza prescrizione del rispetto di tutte le misure e gli accorgimenti prescritti Autorita' Garante come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a

	documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - PROCEDURA OPERATIVA (PO): definire e attuare procedura operativa per dare attuazione, nell'attivita' di videosorveglianza, al principio di c.d. proporzionalita' nella scelta delle modalita' di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonche' nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalita' perseguite - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Produzione di informazione statistica per il perseguimento delle finalita' istituzionali e in conformita' dell'ambito istituzionale del Comune, fatte salve le specifiche normative di settore.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 29 - Trattamento di dati relativi al rilascio delle licenze e autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza
Settore	Settore 2 - Servizi alla Persona
Servizio	2.1 - Turismo, Manifestazioni e Promozione
Ufficio: denominazione e punti di contatto	Ufficio Suolo Pubblico (sezione amministrativa)
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di

	climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei

	dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Concessioni di suolo pubblico per svolgimento di attivita' produttive o no profit e/o eventi.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.2 - Servizio Entrate e Tributi
Ufficio: denominazione e punti di contatto	Ufficio TARSU/TARES/TARI
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gestione, riscossione e controllo tassa sui rifiuti TARES/TARI

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 14 - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Territorio
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	Ambito Territoriale Sociale 16

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gestione delle emergenze sanitarie e delle misure sanitarie, socio-assistenziali, economiche, fiscali, di prevenzione e di sostegno previste dalla legge, dai regolamenti e/o imposte dalle Autorita' competenti a gestire l'emergenza

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 25 - Trattamento di dati relativi alla gestione delle procedure sanzionatorie
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Territorio
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamento violazioni stradali

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 26 - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Territorio
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamento violazioni stradali
Pattugliamento stradale
Ritiro documenti
Interventi per il contrasto del randagismo
Cooperazione con altre forze dell'ordine
Assistenza organi istituzionali: Servizio ordine consiglio comunale
Anagrafe canina
Servizi rappresentanza in celebrazioni e manifestazioni
Recupero veicoli abbandonati su area pubblica
Recupero veicoli rubati trovati in sosta
Concessioni per occupazione temporanee di suolo pubblico - Controllo

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 27 - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Territorio
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sospensione attivita'

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Territorio
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sorveglianza degli attraversamenti pedonali davanti alle scuole
Interventi per manifestazioni, feste, processioni, mercati e manifestazioni sportive
Servizi per obiettivi sensibili
Avvisi di accertamento violazione
Servizio di videosorveglianza

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Territorio
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Acquisizione/messa in funzione apparecchiature per controllo dei veicoli non assicurati, non revisionati, rubati

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 04 - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile
Settore	Settore 3 - Economico e Finanziario
Servizio	3.4 - Servizi Complementari
Ufficio: denominazione e punti di contatto	Ufficio Toponomastica
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Toponomastica Attribuzione numero civico.

Toponomastica Denominazione nuove strade e piazze.

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 38 - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.2 - Servizio Entrate e Tributi
Ufficio: denominazione e punti di contatto	Ufficio Tributi
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Provvedimenti in autotutela per tributi comunali

Servizio informativo risposte a istanze, comunicazioni, richieste di informazioni opposizioni

Rimborsi a contribuenti - riversamenti a Comuni competenti - sgravi di quote indebite e inesigibili di tributi comunali

Istanze interpello

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 3 - Economico e Finanziario
Servizio	3.2 - Servizio Entrate e Tributi
Ufficio: denominazione e punti di contatto	Ufficio Tributi
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo Imposta di soggiorno

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 37 - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati
Settore	Settore 2 - Servizi alla Persona
Servizio	2.1 - Turismo, Manifestazioni e Promozione
Ufficio: denominazione e punti di contatto	Ufficio Turismo
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Concessioni discrezionali non vincolate di contributi, benefici, esoneri e sovvenzioni (Provvedimenti amministrativi discrezionali nell'an e nel contenuto)

Concessione contributi per manifestazioni

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 39 - Trattamento di dati relativi alle attivita' ricreative, di promozione dei giovani.
Settore	Settore 2 - Servizi alla Persona
Servizio	2.1 - Turismo, Manifestazioni e Promozione
Ufficio: denominazione e punti di contatto	Ufficio Turismo
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Autorizzazione per eventi e manifestazioni negli impianti sportivi

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
Settore	Settore 2 - Servizi alla Persona
Servizio	2.1 - Turismo, Manifestazioni e Promozione
Ufficio: denominazione e punti di contatto	Ufficio Turismo
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - APPARECCHIATURE-ICT: attacchi informatici/azione di virus/codici maligni - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle

	specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure

	minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA INCIDENTI: crimeware (malware che mirano a ottenere il controllo dei sistemi) - CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento -TRATTAMENTI ELETTRONICI: utilizzo di parole chiave non adeguate - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e

	relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non

	autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - Tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003 - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del

	trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

**ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Concessione a titolo gratuito delle sale e immobili del patrimonio comunale

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 25 - Trattamento di dati relativi alla gestione delle procedure sanzionatorie
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Verbali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	Maggioli S.p.A. P.Iva 02066400405 Fisso: 0541 628111 Mail: maggiolispa@maggioli.it PEC: segreteria@maggioli.legalmail.it
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rateizzazione sanzioni amministrative

Ordinanze di confisca e provvedimenti di dissequestro

Annullamento d'ufficio verbali per violazioni a norme di Legge.

Ordinanza di ingiunzione

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 30 - Trattamento di dati relativi all'attivita' di consulenza giuridica, nonche' al patrocinio ed alla difesa in giudizio dell'amministrazione nonche' alla consulenza e copertura assicurativa in caso di responsabilita' civile verso terzi dell'amministrazione
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Verbali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i	

trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

	relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gestione del contenzioso udienze G. d. P

Gestione del contenzioso in proprio: elaborazione controdeduzioni per GdP

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42- Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di sopralluogo (Obbligo DPIA)
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Verbali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Emissioni ruoli riscossione sanzioni

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 43 - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche (Obbligo DPIA)
Settore	Settore 1 - Affari Generali
Servizio	1.3 - Corpo di Polizia Municipale
Ufficio: denominazione e punti di contatto	Ufficio Verbali
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle

	pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la

	completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare,

	con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rimborso somme versate erroneamente per violazioni amministrative

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale contrattualizzato presso il Comune (Obbligo DPIA)
Settore	Settore 4 - Tecnico
Servizio	4.3 - Servizio Verde - Arredo Urbano
Ufficio: denominazione e punti di contatto	Ufficio Verde pubblico
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico

	allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalità del controllo, custodia e restituzione della documentazione; d) le modalità del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rilevazione presenze personale

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

**DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA**
(da esibire su richiesta dell'Autorita' di controllo)

ALLEGATO N. XX

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGD
Numero di versione	002
Data ultimo aggiornamento	11/07/2023
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA - Conservazione con supporto informatico

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 27 - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria
Settore	Settore 4 - Tecnico
Servizio	4.1 - Servizio Urbanistica - Edilizia Privata - SUAP
Ufficio: denominazione e punti di contatto	Ufficio Vigilanza Urbanistico Edilizia
Titolare trattamento: denominazione e punti di contatto	Comune di ALASSIO Legale Rappresentante - Sindaco pro tempore fisso: 0182 6021 mail: sindaco@comune.alassio.sv.it
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benché abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati

	- MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione

	alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI
ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamento di conformita' per la sanatoria degli abusi edilizi