PIANO DELLA SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

Il presente documento, in attuazione di quanto previsto dalle Linee guida, riporta il piano della sicurezza del sistema di gestione informatica dei documenti (SdPG) elaborato nel rispetto delle:

- misure di sicurezza predisposte dall'AgID e dagli altri organismi preposti;
- disposizioni in materia di protezione dei dati personali in linea con l'analisi del rischio fatta;
- indicazioni in materia di continuità operativa dei sistemi informatici predisposti dall'AGID.

1. Obiettivi del piano della sicurezza informatica dei documenti

Il piano della sicurezza è finalizzato a garantire che:

- i documenti e le informazioni trattate dall'Ente siano disponibili, integre e riservate tramite l'adozione di idonee misure di sicurezza;
- i dati personali, ivi comprese le categorie particolari di dati personali di cui agli artt. 9 e 10 del Regolamento UE 679/2016 (GDPR), vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

2. Contesto di riferimento

Il SdPG è ospitato presso il Data Center regionale, gestito dalla società in house Insiel s.p.a., nominata quale Responsabile del trattamento ex art. 28 del GDPR, pertanto il piano della sicurezza prevede due componenti, una relativa ad Insiel s.p.a., quale produttore e gestore del SdPG e Responsabile del trattamento, ed una relativa all'Ente, quale Titolare del trattamento e fruitore del SdPG.

Il Piano della sicurezza si basa sull'analisi dei rischi a cui sono esposti i dati e i documenti trattati e rispetta le indicazioni fornite a livello nazionale dall'AgID.

Nello specifico il piano della sicurezza descrive:

- le misure di sicurezza relative alle componenti organizzativa, fisica, logica e infrastrutturale adottate da Insiel s.p.a. e dall'Ente nel contesto della gestione documentale;
- le modalità di funzionamento del SdPG e di accesso ai documenti in esso contenuti;
- le misure specifiche adottate in materia di protezione dei dati personali, ai sensi dell'art. 32 del GDPR, e la procedura da adottarsi in caso di violazione dei dati personali ai sensi degli artt. 33-34 del GDPR da parte di Insiel s.p.a. e dall'Ente;

L'allegato 1 al presente documento riporta "Analisi dei rischi e misure di sicurezza informatica adottate" mentre l'allegato 2 riporta "Analisi dei rischi nell'ambito della gestione documentale e misure organizzative e tecniche adottate".

Le misure descritte sono oggetto di monitoraggio periodico in merito alla loro efficacia ed efficienza.

Il piano della sicurezza è soggetto a revisione con cadenza almeno biennale e può essere modificato a seguito di eventi gravi.

3. Misure minime di sicurezza in ambito ICT

In attuazione di quanto previsto dalla Circolare AgID 18 aprile 2017, n. 2, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni", l'Ente ha approvato e attuato il documento "Allegato 2.3 - misure minime sicurezza ICT" allegato 3 al presente documento.

Tali misure possono essere oggetto di riesame in conseguenza del verificarsi di incidenti attinenti alla sicurezza,

di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza, che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza, portare alla modifica del livello di sicurezza complessivo o ad aggiornamenti delle prescrizioni minime di sicurezza richieste dall'AgID; il riesame può avvenire anche a seguito dei risultati delle attività di audit esterno.

4. Componente organizzativa della sicurezza

Insiel s.p.a. si avvale di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) certificato secondo la norma UNI EN ISO/IEC 27001:2017 che contiene i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni dal punto di vista della sicurezza logica, fisica/ambientale e organizzativa; inoltre il SGSI rispetta le linee guida ISO/IEC 27017, in relazione alla protezione dei servizi erogati in modalità cloud, nonché alla linea guida ISO/IEC 27018, in relazione alla protezione delle informazioni ascrivibili a dati personali, sempre nell'ottica dell'erogazione di servizi cloud; il SGSI comprende, nel suo ambito di applicazione, le infrastrutture di sicurezza fisica e logica del Data Center.

In attuazione di quanto previsto dagli standard sopra citati, Insiel s.p.a. ha individuato e definito formalmente ruoli e responsabilità che comprendono la figura del Responsabile del SGSI e diversi soggetti responsabili dell'implementazione e dell'adozione delle misure di sicurezza.

È presente un processo di governo degli eventi rilevanti per la sicurezza che prevede la rilevazione, la gestione di tali eventi, la risoluzione degli incidenti, la raccolta degli spunti per il miglioramento.

Il personale specializzato sui temi della sicurezza informatica contempla tecnici certificati ISO 27001 (Sistemi di gestione della sicurezza delle informazioni), CISSP (Certified Information Systems Security Professional) e CISM (Certified Information Security Manager).

La componente organizzativa della sicurezza afferente all'Ente è gestita attraverso servizi esternalizzati, competenti in materia di sistemi informativi.

5. Componente fisica della sicurezza

La sede che ospita il Data Center soddisfa i requisiti di cui al d.lgs. n. 81/2008 recante la *"Tutela della salute e della sicurezza nei luoghi di lavoro"*.

L'accesso fisico è controllato, i dipendenti utilizzano badge magnetici per gli ingressi e gli ospiti devono venir identificati. Le aree esterne sono sorvegliate da un sistema televisivo a circuito chiuso mediante telecamere dislocate lungo il perimetro; le uscite di sicurezza sono controllate da sensori a contatto che rilevano intrusioni o anomalie.

È, inoltre, presente un controllo regolare di ronda notturna da parte di un servizio di Guardie Giurate che integra il presidio operativo, comunque presente 24 ore su 24; l'accesso ai locali tecnici è permesso solamente al personale autorizzato. L'intera area è protetta da un impianto automatico di controllo fumi e spegnimento automatico a gas.

L'accesso fisico alle sedi dell'Ente è controllato, i dipendenti utilizzano badge magnetici per gli ingressi e gli ospiti devono venir identificati.

La sede principale dell'Ente è dotata di un sistema di telecamere che controlla il perimetro esterno e presenta un servizio di guardiania o di portierato. Le stanze dove ha luogo la protocollazione, alla fine del turno di lavoro, vengono chiuse a chiave.

6. Componente logica della sicurezza

La componente logica della sicurezza è ciò che garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Per gli utenti interni all'Amministrazione, l'accesso al SdPG avviene, per le applicazioni di tipo web, per mezzo

del trasferimento automatico delle credenziali utente acquisite al momento dell'autenticazione al dominio, mentre, per le applicazioni di tipo client / server, per mezzo di codice utente e password.

Viene richiesta la modifica della password al momento del primo accesso al sistema ed allo scadere di sei mesi dall'ultima variazione; il mancato accesso ad un sistema applicativo per un periodo superiore ai sei mesi comporta la decadenza delle credenziali dell'utente interessato che deve richiederne la riattivazione.

Nel SdPG sono presenti, per ogni utente, le informazioni che determinano la disponibilità delle funzioni applicative e la possibilità di accedere ai dati ed ai documenti archiviati nel sistema.

I soggetti esterni accedono, di norma, ai servizi online di acquisizione di istanze tramite il Sistema pubblico per la gestione delle identità digitali –SPID, la Carta d'Identità Elettronica o la Carta Nazionale dei Servizi, in attuazione di quanto previsto dal d.lgs. 82/2005 recante il Codice dell'Amministrazione Digitale.

Il sistema è ospitato nel Data Center regionale dove:

- è presente una struttura di accesso ad Internet a più livelli, separati dai dispositivi firewall. Inoltre, sono implementate politiche di segmentazione delle reti in contesti logici diversi a seconda delle caratteristiche dei servizi erogati;
- sono in uso sistemi IDS (Intrusion Detection System) e IPS (Intrusion Prevention System);
- esiste un presidio attivo 24 ore su 24 che provvede alle attività necessarie a garantire la regolare operatività dei servizi;
- è presente un sistema di backup dei dati. In particolare, viene eseguito un backup completo del Database ogni settimana ed uno incrementale ogni notte;
- i sistemi utilizzano dispositivi di ridondanza.

Inoltre Insiel s.p.a. è dotata di un Sistema di Gestione della Continuità Operativa, che è oggetto di audit periodico, sia interno che di terza parte, ed è certificato secondo la norma EN ISO 22301:2012 relativa alla gestione della continuità operativa.

7. Componente infrastrutturale della sicurezza

Presso il Data Center regionale sono disponibili i seguenti impianti che costituiscono la componente infrastrutturale della sicurezza:

- uscite di sicurezza;
- luci di emergenza;
- sistema di videosorveglianza;
- guardiola all'ingresso presidiata da guardie giurate;
- sensori antintrusione;
- controllo degli accessi e dei varchi fisici;
- sistema di controllo dei fumi e spegnimento automatico a gas Inergen;
- continuità elettrica.

Gli impianti e le considerazioni precedenti valgono anche per la componente infrastrutturale della sicurezza dell'Ente, coerentemente con il livello di criticità di ciascuna sede.

8. Gestione degli accessi al SdPG e al Database

Il SdPG registra gli accessi da parte degli utenti e le attività riferibili all'attribuzione ed alla modifica delle password ed alla riattivazione di credenziali scadute.

Vengono altresì memorizzate le attività di aggiornamento dei dati di protocollo con evidenza dell'utente che le ha effettuate e, per quanto riguarda i dati essenziali, con registrazione della versione precedente dell'informazione.

Le registrazioni degli accessi da parte degli Amministratori di Sistema vengono effettuate con l'impiego di

un'apposita infrastruttura tecnologica che garantisce l'accesso mediante credenziali di autenticazione individuali ed è volto a garantire:

- la registrazione degli accessi (access log) ai sistemi di elaborazione e agli archivi elettronici, comprendenti i riferimenti temporali e la descrizione dell'evento che le ha generate;
- che le registrazioni possiedano caratteristiche di completezza e inalterabilità;
- che le registrazioni vengano conservate per un periodo non inferiore ai sei mesi.

Con le medesime modalità vengono eseguite le registrazioni degli accessi degli Amministratori di Sistema al Database.

Viene, infine, eseguito un backup completo del Database ogni settimana ed uno incrementale ogni notte.

9. Strumenti per la trasmissione e l'interscambio dei documenti informatici

La trasmissione dei documenti informatici avviene principalmente tramite posta elettronica certificata, le caselle PEC di cui si avvale l'Ente sono rilasciate da un fornitore esterno certificato (Gestore – per il tramite della Regione), che fornisce garanzie che vengono considerate dall'Amministrazione idonee dal punto di vista della sicurezza.

Fra le principali misure di sicurezza che vengono adottate per garantire che le attività del Gestore si svolgano secondo i requisiti di sicurezza richiesti dalla normativa vigente, si ricordano:

- I meccanismi per il controllo dell'accesso logico e fisico alle risorse informatiche e ai sistemi del Gestore, che forniscono le seguenti funzionalità:
 - identificano ed autenticano le persone autorizzate ad accedere alle risorse informatiche;
 - impediscono ad una persona non autorizzata di poter accedere alle risorse informatiche;
 - registrano i dati significativi di tutti gli eventi di accesso in modo che si possa in ogni caso risalire alla persona che ha dato origine ad un determinato evento.
- Il controllo dell'accesso ai locali protetti adotta una politica di autorizzazioni e di procedure di registrazione e auditing:
 - l'accesso alla Sala Sistemi del Centro Servizi del Gestore è basato sul principio secondo il quale è consentito l'accesso solo a chi è esplicitamente autorizzato:
 - ogni persona che intende accedere alle risorse della Sala Sistemi è identificata in modo certo, mediante l'utilizzo di una smartcard o un token personale.
 - ogni operazione di firma di messaggi, avvisi e ricevute svolta dal sistema di posta certificata viene tracciata in un registro di controllo al quale viene associata con periodicità almeno giornaliera una marca temporale.

10. Accesso ai documenti informatici e gestione delle abilitazioni

L'accesso ai documenti informatici è effettuato mediante il SdPG, con le modalità di seguito descritte.

10.1. Utenti interni all'Ente

L'accesso al SdPG è consentito solamente agli utenti esplicitamente autorizzati e la fruizione di funzioni ed informazioni è condizionata dal tipo di abilitazione attribuita ad ogni utente.

Le abilitazioni vengono attribuite per mezzo di apposite funzioni messe a disposizione del SdPG e vengono richieste e formalizzate secondo le modalità descritte di seguito.

Gli utenti vengono, di norma, associati ad uno o più gruppi funzionali ai quali sono stati attribuiti specifici diritti di accesso, registrazione, modifica, annullamento su uno o più registri di protocollo, generale o particolare. Gli utenti ereditano le caratteristiche proprie dei gruppi funzionali a cui sono associati.

In più, per ogni utente, possono essere definite specifiche abilitazioni che determinino ulteriori diritti rispetto a quelli dei gruppi funzionali di appartenenza.

La fruizione delle registrazioni di protocollo è consentita agli utenti ai quali, in modo diretto oppure in quanto appartenenti ad una struttura, sia stato attribuito uno specifico diritto di accesso. Ciò può avvenire o perché l'utente o la struttura sono gli autori del documento, oppure perché risultano essere assegnatari di un documento pervenuto, oppure perché partecipano ad un flusso di lavorazione interno.

È possibile definire strutture alle quali vengano assegnati utenti che, in virtù del loro ruolo istituzionale o delle loro mansioni, accedono alla totalità delle registrazioni di uno o più registri.

Le abilitazioni o disabilitazioni dei dipendenti dell'Amministrazione devono essere richieste da un funzionario responsabile di Servizio al responsabile della gestione documentale tramite l'invio di una mail.

Le richieste devono necessariamente riportare le seguenti informazioni:

A) Se richiesta di abilitazione:

- Descrizione richiesta: Abilitazione a protocollo e/o visura protocollo e/o iteratti;
- Utente: Matricola / Cognome / Nome;
- Struttura/e alla quale l'utente va assegnato: codice della struttura / descrizione della struttura così come definiti nel sistema di protocollo, con l'indicazione della struttura primaria;
- Dicitura: La presente richiesta di abilitazione sostituisce oppure integra le abilitazioni eventualmente già attribuite all'utente

B) Se richiesta di disabilitazione:

- Descrizione richiesta: Disabilitazione a protocollo e/o visura protocollo e/o iteratti;
- Utente: Matricola / Cognome / Nome
- Struttura/e dalla quale l'utente va rimosso: codice struttura.

Il responsabile della gestione documentale provvede alla valutazione delle richieste e, in caso positivo, le approva e le inoltra all'Insiel s.p.a. per l'esecuzione.

Ogni utente abilitato ad accedere al SdPG viene configurato per quanto riguarda:

- le funzioni di cui può fruire (protocollazione in arrivo/partenza, interrogazioni, firma digitale, ed altro);
- le registrazioni su cui vengono attribuiti i diritti di gestione o visibilità.

Gli utenti ereditano le abilitazioni attribuite alle rispettive strutture di appartenenza.

Nel caso in cui, a seguito di modifiche dell'organizzazione interna dell'Amministrazione, si renda necessario istituire nuove strutture o modificare la configurazione di strutture esistenti tale richiesta dovrà essere inoltrata con le medesime modalità.

Le richieste devono necessariamente riportare le seguenti informazioni:

- Creazione di una nuova struttura:
 - codice struttura (proposta);
 - denominazione struttura.
- Configurazione struttura:
 - codice e denominazione delle strutture esistenti eventualmente collocate a livello gerarchico superiore;
 - codice e denominazione delle strutture esistenti o nuove eventualmente collocate a livello gerarchico inferiore;
 - diritti di visibilità rispetto ai documenti di pertinenza di strutture di cui ai punti precedenti;
- Codice AOO e codice registro su cui la struttura può operare.

In alternativa, è possibile indicare codice e descrizione di una struttura la cui configurazione deve essere replicata sulla struttura interessata.

Poiché le abilitazioni di visura sono legate all'associazione ad una o più strutture, le stesse vengono meno al momento della rimozione dell'associazione del dipendente dalle strutture stesse. Restano visibili le registrazioni in cui l'utente ha avuto parte attiva (creazione, trattamento in iter).

Al fine di mantenere un controllo efficiente ed efficace in materia di accesso alle informazioni ed ai sistemi, il Servizio per la gestione documentale esegue dei controlli a campione al fine di verificare la rispondenza tra abilitazioni possedute e struttura di appartenenza e un controllo semestrale sulla disabilitazione del personale cessato.

10.2. Utenti esterni all'Ente - Amministrazioni

Sono in fase di studio da parte dell'Ente funzioni che permettano l'accesso diretto ai documenti da parte di altre Amministrazioni.

10.3. Utenti esterni all'Ente - Privati

Sono in fase di studio da parte dell'Ente funzioni per l'esercizio, per via telematica, del diritto di accesso ai documenti da parte di privati cittadini.

11. Protezione dei dati personali

La gestione dei flussi documentali e il SdPG sono ispirati alle norme in materia di tutela dei dati personali, con particolare riferimento al concetto di accountability ed alla capacità di adottare un processo efficace per la protezione degli stessi in grado di ridurre al minimo i rischi di una loro possibile violazione.

In merito al trattamento dei dati personali, Insiel s.p.a. agisce in qualità di Responsabile del trattamento ai sensi dell'art. 28 del GDPR ed attua gli adempimenti previsti con particolare riguardo a:

- Tenuta di un registro delle attività di trattamento in qualità di Responsabile.
- Rispetto delle istruzioni ricevute dal Titolare nell'atto di designazione a Responsabile del trattamento.
- Adozione delle misure di sicurezza previste sulla base dell'analisi dei rischi di cui all'allegato 1 tra cui:
 - misure per assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento tramite il SGSI di cui si è dotata la Società;
 - misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, tramite il Sistema di Gestione della Continuità operativa di cui si è dotata la Società;
 - procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento: secondo quanto previsto dallo standard internazionale ISO27001, è previsto che siano condotti, ad intervalli pianificati, audit interni per fornire informazioni tali da permettere di riconoscere se il SGSI è conforme allo standard di riferimento adottato;
 - misure di protezione dei dati durante la trasmissione: nelle reti vengono previste delle configurazioni atte a segregare gruppi di servizi, di utenti e di sistemi informativi, secondo i requisiti previsti;
 - misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati, progettando e applicando la sicurezza fisica agli uffici, ai locali ed agli impianti ove avviene il trattamento di dati personali. Le apparecchiature vengono disposte e protette al fine di ridurre i rischi derivanti dalle minacce e dai pericoli ambientali, oltre alle occasioni di accesso non autorizzato;
 - misure per limitare l'accesso ai dati esclusivamente al personale autorizzato, tramite sistemi di autenticazione;
 - misure per garantire la registrazione degli eventi di accesso da parte degli Amministratori di Sistema, secondo quanto previsto dal Provvedimento del Garante del 27.11.2008 e in base alle istruzioni ricevute dal Titolare;
 - misure per garantire la responsabilità: la Società identifica per iscritto i propri dipendenti deputati a trattare i Dati Personali tramite apposite lettere di incarico, individuando l'ambito di trattamento consentito e fornendo loro le istruzioni idonee allo scopo, in particolare vincolandoli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il

periodo successivo alla cessazione del rapporto di lavoro. La Società ne cura la formazione, vigila sul loro operato e comunica all'Ente, su specifica richiesta, l'elenco aggiornato degli stessi. La Società designa quali Amministratori di Sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali; predispone e conserva l'elenco contenente gli estremi identificativi degli Amministratori di Sistema e le funzioni ad essi attribuite; comunica all'Ente, su specifica richiesta, tale elenco aggiornato; verifica annualmente il loro operato. La Società, qualora si avvalga di fornitori terzi per eseguire le attività di trattamento, provvede a designarli sub-responsabili del trattamento, imponendo i medesimi obblighi cui è tenuta ad adempiere in qualità di Responsabile ex art. 28 GDPR e comunica i nominativi dei fornitori all'Ente.

- Per i trattamenti di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati (artt. 9 e 10 GDPR), adozioni di limitazioni e garanzie che tengono pienamente conto della natura dei dati e dei rischi connessi, quali il trattamento dati permesso solo per le finalità prestabilite dal Titolare, limitazioni all'accesso ai dati, limitazioni all'accesso fisico ai locali in cui i dati personali sono trattati, accesso con autenticazione, autorizzazione per iscritto del personale che accede ai dati, dotato di formazione specializzata e tenuto all'obbligo di riservatezza; registrazione degli eventi con conservazione dei log di accesso ai dati da parte degli amministratori di sistema per almeno 6 mesi; applicazione di misure per limitare trasferimenti successivi dei dati; trattamento dei dati esclusivamente nel territorio dell'Unione Europea; misure per garantire la continuità operativa al fine di assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
- In caso di violazione dei dati personali, collaborazione e supporto al Titolare nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del GDPR, tenuto conto della natura del trattamento e delle informazioni a disposizione della Società.
- In caso di una violazione dei dati personali trattati dal Titolare, collaborazione e supporto al Titolare:
 1. nel notificare la violazione dei dati personali all'autorità di controllo competenti, senza ingiustificato ritardo dopo che il Titolare ne è venuto a conoscenza, se del caso (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
 2. nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del GDPR, devono essere indicate nella notifica del Titolare e includere almeno:
 - la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
 - le probabili conseguenze della violazione dei dati personali;
 - le misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo;

3. nell'adempiere, in conformità all'articolo 34 del GDPR, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

- In caso di una violazione dei dati personali trattati dalla Società in qualità di Responsabile, invio di una notifica al Titolare senza ingiustificato ritardo contenente almeno:
 1. una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
 2. i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
 3. le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

L'Ente agisce in qualità di Titolare ed attua gli adempimenti previsti dal GDPR con particolare riguardo a:

- Tenuta di un registro delle attività di trattamento.
- Nomina dei Responsabili del trattamento con indicazione precisa dei comportamenti a cui attenersi nel rispetto di quanto previsto dall'art. 28 del GDPR.

Inoltre, al fine di mitigare le minacce individuate nell'analisi dei rischi di cui all'allegato 2 e garantire la riservatezza dei dati trattati, l'Amministrazione ha adottato, oltre alle misure già descritte nei paragrafi precedenti, i seguenti ulteriori accorgimenti:

- impartire istruzioni al personale autorizzato ad accedere al SdPG quali:
 - trattare i dati personali in modo lecito e secondo correttezza;
 - raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
 - verificare che tali dati siano esatti e, se necessario, provvedere all'aggiornamento;
 - comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati a riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti;
 - astenersi dal comunicare a terzi, al di fuori dell'ambito lavorativo, qualsivoglia dato personale;
 - informare tempestivamente il Titolare del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;
 - accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
 - non fornire dati e informazioni relativi a terzi, senza una specifica autorizzazione del Titolare;
 - non fornire dati e informazioni ai diretti interessati, senza avere la certezza della loro identità;
 - quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, ritirare tempestivamente i documenti stampati per evitare che soggetti non abilitati al trattamento ne prendano visione.
 - non salvare documenti contenenti dati personali sulle risorse locali (hard disk della postazione pc o del notebook o comunque di qualsiasi dispositivo aziendale) o su dispositivi di memorizzazione esterni (hard disk esterni, chiavette usb) o ancora su dvd/cd-rom;
 - a fine turno di lavoro, cancellare dalle risorse locali (e svuotare il cestino) eventuali file contenenti dati personali, facendo attenzione alla cartella "Download" o alla cartella dove vengono scaricati i file dal browser;
 - non comunicare ad altri o dare evidenza delle credenziali di accesso al proprio computer e agli applicativi in uso;
 - in caso di assenza momentanea dalla propria postazione accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone chiudendo la sessione di lavoro attraverso

la disconnessione (logout) oppure, in alternativa, attivando un salvaschermo protetto dalle credenziali di autenticazione.

- spegnere il proprio computer al termine delle ore di servizio.
- impartire istruzioni specifiche al personale addetto alla protocollazione quali:
 - smistare i documenti solo al gruppo funzionale del responsabile della struttura interna competente alla trattazione del procedimento a cui il documento si riferisce;
- impartire istruzioni al personale nella gestione della documentazione cartacea quali:
 - non lasciare incustoditi i documenti contenenti dati personali nello svolgimento dell'attività lavorativa e al termine del turno di lavoro conservarli in archivi ad accesso controllato, al fine di escludere l'accesso agli stessi da parte di persone non incaricate al trattamento;
 - conservare la documentazione contenente le categorie particolari di dati personali di cui agli artt. 9 e 10 del GDPR in armadi muniti di serratura, al fine di escludere l'acquisizione o la presa visione degli stessi, da parte di persone non incaricate al trattamento;
 - qualora sia necessario distruggere i documenti contenenti dati personali, utilizzare gli appositi apparecchi "distruggi documenti" o, in assenza, sminuzzare i documenti in modo da non essere più ricomponibili;
 - nella movimentazione o trasmissione dei documenti all'interno dell'Amministrazione adottare idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in contenitori o buste chiuse).
- limitare le informazioni relative a stati, fatti e qualità personali contenute nei documenti trasmessi all'interno dell'Amministrazione o a soggetti esterni a quelle che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse;
- adozione di un sistema di sicurezza che nello svolgimento delle attività di registrazione di protocollo garantisca la protezione dei dati personali registrati in base all'architettura del sistema informativo, ai controlli sull'accesso e ai livelli di autorizzazione previsti, come descritto nei capitoli precedenti.

Inoltre, in attuazione di quanto previsto dall'art. 46 del CAD, al fine di garantire la riservatezza dei dati particolari di cui agli artt. 9 e 10 del GDPR, i documenti informatici trasmessi ad altre pubbliche amministrazioni per via digitale possono contenere soltanto i dati sensibili e giudiziari consentiti da legge o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisiti.

In caso di violazione dei dati personali ai sensi degli artt. 33 e 34 del GDPR, l'Ente segue le procedure descritte nel documento "Allegato 2.4 - regole data breach", allegato 4 al presente documento.

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: CHITTARO MICHELA

CODICE FISCALE: CHTMHL81E65L483T

DATA FIRMA: 02/07/2025 13:16:04

IMPRONTA: 4D1358A31D1F1332EBA874D5D8CE27D2136907FC98B52D6E84D559FD83C093B5
136907FC98B52D6E84D559FD83C093B54C591BFF4E3E742F282D844BCAA545B3
4C591BFF4E3E742F282D844BCAA545B3F6F43CFEDAC92C28E1E71263558CDBF2
F6F43CFEDAC92C28E1E71263558CDBF2B8FD13E568130145BD0D54DF46DE0444