COMUNE DI SERRAVALLE SCRIVIA

VIA BERTHOUD 49
15069 Serravalle Scrivia (AL)
P.IVA 00211750062

DATA PROTECTION IMPACT ASSESSMENT - Ai sensi art. 35 del Regolamento Europeo 2016/679

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, adottate e da adottare per il trattamento dei dati personali effettuato da COMUNE DI SERRAVALLE SCRIVIA per una valutazione dell'impatto sui trattamenti.

Misure Logiche e Organizzative

Le seguenti misure organizzative sono da considerarsi su tutta l'organizzazione Aziendale

Misure Adottate

- **Redazione di un piano di formazione per gli addetti**
- **Verifica periodica dell'ambito dei trattamenti e dei profili di autorizzazione.**
- **Verifica dei Back-up.**
- **Consegna istruzioni dettagliate agli addetti.**
- **Procedure per ripristino dei dati.**
- **È stato redatto e viene annualmente aggiornato il Manuale Organizzativo Privacy.**
- **Descrizione scritta degli interventi effettuati da terzi.**
- **Individuazione estremi identificativi delle persone fisiche preposte quali amministratori di sistema dell'azienda di outsourcing esterna.**
- **Verifica annuale operato Amministratori di Sistema.**
- **Redazione del Registro dei Trattamenti sia in qualità di Titolare sia se necessario in qualità di Responsabile**
- **Redazione documento Privacy by Design e By Default**
- **Nomina del DPO**
- **Procedure Gestione Data Breach**
- **Implementazione Procedura di Nomina a Responsabile del trattamento**
- **Implementazione procedura di verifica per i Responsabile del trattamento**
- **Verifica delle valutazioni preventive ai sensi dell'art. 5 paragrafo 1 del GDPR.**

Misure previste dal piano di mitigazione dei Rischi

- **Consegna istruzioni dettagliate agli addetti.**
  - **Istruzioni per la segretezza del sistema di autenticazione e la custodia dei dispositivi personali.**
  - **Istruzioni per i supporti removibili in caso di dati sensibili o giudiziari.**

Elenco per trattamento

I rischi associati ai trattamenti sono la somma pesate dei rischi logici ed organizzativi sui dati e dei rischi presenti sugli archivi utilizzati per il trattamento.

- **Whistleblowing**

  Fattore di rischio residuo dopo valutazione di impatto **2/10** **(Basso)**

  Gestione dei dati personali forniti da soggetti che segnalino illeciti per l'analisi e la gestione della segnalazione, nonché per l'accertamento dei fatti oggetto della segnalazione e adozione dei conseguenti provvedimenti, in adempimento delle previsioni di cui al D. Lgs. 10 marzo 2023, n. 24

Livello di copertura:	• Fattore di rischio iniziale: 9/10 • Fattore di rischio residuo: 2/10 • Percentuale di copertura tramite misure attuate: 79% • Percentuale di copertura tramite misure da attuare dopo valutazione di impatto: 79%
Dati Comuni trattati:	• nominativo, indirizzo o altri elementi di identificazione personale.
Dati Particolari trattati:	• Dati comuni ed eventuali dati particolari trattati nell'ambito della gestione delle segnalazioni whistleblowing.
Archivi utilizzati per il trattamento	• WhistleblowingPA .

Interessati al trattamento, finalità e base giuridica

► **Segnalante whistleblowing**	• rivelazione della sua identità a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni (comma 2 dell'art. 12 D.Lgs 24/2023) o nell'ambito del procedimento, ove la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza della sua identità sia indispensabile per la difesa dell'incolpato (comma 5 dell'art. 12 D.Lgs 24/2023). [richiesta di consenso]. • Attività di compliance in ambito D.Lgs 24/2023 [obbligo di legge o contrattuale]. • Ricezione, analisi e gestione della segnalazione, nonché per l'accertamento dei fatti oggetto della stessa e adozione dei conseguenti provvedimenti, in adempimento delle previsioni di cui al D. Lgs. 10 marzo 2023, n. 24 [obbligo di legge o contrattuale].

Rischio di Disponibilità dei dati

► **Mancata disponibilità dei dati**	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
► **Eliminazione o perdita dei dati al di fuori dell'ambito definito**	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO

Rischio di Integrità dei dati

► **Modifica errata o mancato aggiornamento dei dati**	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
► **Trattamento dei dati secondo modalità differenti da quelle dichiarate**	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO

Rischio di Riservatezza dei dati

► **Comunicazione dei dati al di fuori dell'ambito definito**	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
► **Diffusione dei dati al di fuori dell'ambito definito**	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
► **Trattamento dei dati al di fuori dell'ambito degli addetti autorizzati**	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO

Accadimenti possibili sugli archivi

Divulgazione Intenzionale dei Dati	Rischio Residuo Livello di Copertura	MOLTO BASSO MEDIO
Errori di trasmissione (incluso il misrouting)	Rischio Residuo Livello di Copertura	MOLTO BASSO ALTO
Furti di Dati perpetrati dall'esterno	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Accesso non autorizzato o Furto di dati personali	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Fault o malfunzionamento della strumentazione IT	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Distruzione di strumentazione da parte di persone malevole	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Eccesso di traffico sulle linee di TLC	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Danni alle linee di TLC	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Saturazione dei sistemi IT	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Divulgazione accidentale dei Dati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Errori di manutenzione hardware e software	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Distruzione o Modifica volontaria dei Dati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Accesso a Sistemi contenenti informazione da parte di addetti non autorizzati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO

Furti di Dati perpetrati da personale Interno	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Furto di Identità degli Addetti	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Presenza di Virus	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Mancato recupero di informazioni da media (principalmente memorie di massa) di backup up	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Furto di apparati o sistemi	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Scrittura Dati errati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Errori non volontari durante modifica o cancellazione di Dati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Distruzione o Modifica accidentale dei Dati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Errore di salvataggio sui supporti di Back-up	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Malfunzionamenti software	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO

Misure Adottate

Misure Fisiche

- **Copie di Back-up.**
  - **Back-Up giornaliero.**
  - **Back-Up eseguito in Automatico.**
  - **Back-Up Incrementale.**
  - **Back-Up su supporti sempre differenti.**
  - **Back-Up in Cloud.**
- **Credenziali di autentificazione, assegnate individualmente ad ogni addetto.**
  - **Autenticazione mediante user-id e password.**
  - **Parola chiave di almeno 8 caratteri.**
  - **Disattivazione delle vecchie credenziali.**
  - **Disposizioni scritte per la disponibilità dei dati.**
- **Cifratura dei dati memorizzati.**
- **Cifratura dei dati trasmessi.**
  - **Cifratura con protocollo SSL.**
- **Sospensione automatica delle sessioni di lavoro.**
- **Sospensione manuale delle sessioni di Lavoro.**
- **Sono stati adottati adeguati criteri tra cui l'eventuale nomina a Responsabile per garantire che la struttura esterna presso cui l'unità di archiviazione risiede abbia adeguate contromisure che garantiscano un rischio residuale basso.**
- **Separazione dei dati sulla salute dagli altri dati personali su sistemi elettronici**

- **Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda**
- **Verifica ed eventuale nomina degli amministratori di sistema se presenti**
- **Pseudonimizzazione.**
- **Trattamento dei dati con protocolli criptati.**
- **Profili di autorizzazione di ambito diverso per diversi incaricati.**
  - **È utilizzato un sistema di autorizzazione.**
  - **I profili di autorizzazione vengono specificati prima di ogni trattamento.**
  - **Verifica periodica del profilo di autorizzazione.**
- **Separazione Fisica delle copie dei dati.**
- **Sicurezza Wall Breakers**

Misure previste dal piano di mitigazione dei Rischi

Misure Fisiche

- **Credenziali di autentificazione, assegnate individualmente ad ogni addetto.**
  - **Autenticazione mediante dispositivo di autenticazione ad uso esclusivo dell'incaricato.**