PROCEDURA
per la
GESTIONE DI UNA VIOLAZIONE DI DATI PERSONALI

Ufficio del RESPONSABILE PROTEZIONE DATI (RPD)

TEL: 0187 534300
Mail: privacy@asl5.liguria.it
PEC: dpo@pec.asl5.liguria.it
WEB: https://www.asl5.liguria.it/privacy.aspx
http://portale.asl5.local/it-it/privacy.aspx

Revisione	Data	Natura della modifica
0	18/08/2023	Prima emissione

Redazione	Revisione 0 del 18/08/23	Responsabile protezione dati	Alessandro Vattovani	Firmato in originale
Verifica Tecnica				
Approvazione		Titolare del trattamento	Dott. Paolo Cavagnaro	Firmato in originale

INDICE

1. FINALITÀ

Il "**REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI** Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016" (nel prosieguo **RGPD**) pone l'accento sulla "responsabilizzazione" (*accountability*) ossia sull'adozione di comportamenti proattivi da parte del **TITOLARE** del trattamento tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del **RGPD**.

Con la presente procedura l'Azienda Sociosanitaria Ligure 5 (ASL 5) quale **TITOLARE** del trattamento comunica agli **INTERESSATI**, ovverosia assistiti, pazienti e utenti, nonché agli **AUTORIZZATI**, ovverosia DIPENDENTI (area del comparto e della dirigenza), CONVENZIONATI (medico e odontoiatra specialista ambulatoriale interno, veterinario e altre professionalità sanitarie, biologo, chimico, psicologo, ambulatoriali) e altri OPERATORI, interni ed esterni, attivi in ASL 5 qualunque sia il sottostante rapporto giuridico (borsista, collaboratore, comandato, contraente di contratto a t.d. di diritto privato, distaccato, interinale, studente, tirocinante, volontario etc.), le modalità per la gestione di una violazione dei dati personali (cd. **DATA BREACH**) prevista agli artt. 33 e 34 del **RGPD**.

Il diritto di ricevere una comunicazione a seguito di una violazione di propri dati personali sarà resa direttamente dal **TITOLARE** del trattamento ASL 5, senza necessità che l'**INTERESSATO/A** ne faccia espressa richiesta, e ciò avverrà quando il **DATA BREACH** è suscettibile di presentare un rischio elevato per i diritti e le libertà dell'**INTERESSATO/A.**

Si definisce **DATA BREACH** una violazione di sicurezza che comporti - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali (non solo "sensibili" e "giudiziari" ma anche "comuni") trasmessi, conservati o comunque utilizzati dal **TITOLARE** ASL 5. Per dati personali "comuni" si intendono quelli anagrafici, di contatto nonché di accesso e identificazione etc. (*cfr. infra amplius*).

Un **DATA BREACH** può compromettere la confidenzialità (diffusione o accesso non autorizzato o accidentale), l'integrità (modifica non autorizzata o accidentale) o la disponibilità (impossibilità di accesso o distruzione non autorizzata o accidentale) di dati personali, digitali o cartacei, nonché qualsiasi combinazione di tali ambiti informativi. Alcuni possibili esempi sono:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, etc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Per preservare confidenzialità e riservatezza dei dati personali, l'**AUTORIZZATO** al trattamento dei dati "*osserva il segreto d'ufficio e la normativa in materia di tutela dei dati personali e qualora sia richiesto di fornire informazioni, atti o documenti non accessibili informa il richiedente dei motivi che ostano all'accoglimento della richiesta. Nessun dirigente o dipendente può rilasciare dichiarazioni alla stampa o a programmi televisivi e non pubblica sui social network pagine riconducibili o riferibili all'Azienda e/o all'attività presso la stessa, senza la preventiva autorizzazione della Direzione Generale. I rapporti coi mezzi di informazione sugli argomenti*

istituzionali sono tenuti dalla Direzione Generale nonché dai dipendenti espressamente incaricati" (*cfr*. vigente Codice di comportamento aziendale).

Scopo della presente procedura è quello di disegnare il flusso informativo per la gestione di una violazione di dati personali occorsa in ASL 5 e rilevata da un **AUTORIZZATO**, interno o esterno, attivo in ASL 5 (qualunque sia il rapporto giuridico), afferente sia al comparto sia alla dirigenza.

È di fondamentale importanza che tutto il Sistema *privacy* aziendale si attivi senza indugio nell'eventualità in cui si presenti una violazione concreta oppure potenziale finanche soltanto sospetta di dati personali, in modo da poter comunicare la violazione entro 72 ore dall'accadimento all'**AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI** e senza ingiustificato ritardo agli **INTERESSATI**, ciò al fine di evitare rischi per i diritti e le libertà delle persone, nonché possibili danni economici all'Azienda.

2. RIFERIMENTI

- **AMMINISTRATORE DI SISTEMA**: l'OPERATORE INFORMATICO, interno o esterno, attivo in ASL 5 (qualunque sia il rapporto giuridico) che si occupa della gestione e della manutenzione di un impianto di elaborazione o di sue componenti, di basi di dati, di reti e di apparati di sicurezza, di sistemi *software* complessi;
- **AUTORITÀ DI CONTROLLO NAZIONALE**: AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
- **AUTORIZZATO**: il DIPENDENTE (area del comparto e della dirigenza), il CONVENZIONATO (medico e odontoiatra specialista ambulatoriale interno, veterinario e altre professionalità sanitarie, biologo, chimico, psicologo, ambulatoriali) o l'OPERATORE, interno o esterno, attivo in ASL 5 qualunque sia il sottostante rapporto giuridico (borsista, collaboratore, comandato, contraente di contratto a t.d. di diritto privato, distaccato, interinale, studente, tirocinante, volontario etc.);
- **DATO PERSONALE**: qualsiasi informazione riguardante una persona fisica identificata o identificabile;
- **DPO**: *Data protection officer* (vedi RPD);
- **GDPR**: *General Data Protection Regulation* (vedi RGPD);
- **INTERESSATO**: la PERSONA (fisica) alla quale si riferiscono i dati trattati da ASL 5;
- **RGPD**: REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;
- **RPD**: Responsabile della protezione dei dati;
- **RESPONSABILE (ESTERNO) DEL TRATTAMENTO**: il fornitore, la struttura accreditata etc. che effettua un trattamento di dati personali degli INTERESSATI per conto del TITOLARE ASL 5;
- **TITOLARE DEL TRATTAMENTO**: ASL 5 in quanto determina finalità e mezzi del trattamento di dati personali degli Interessati;

ESTERNI:

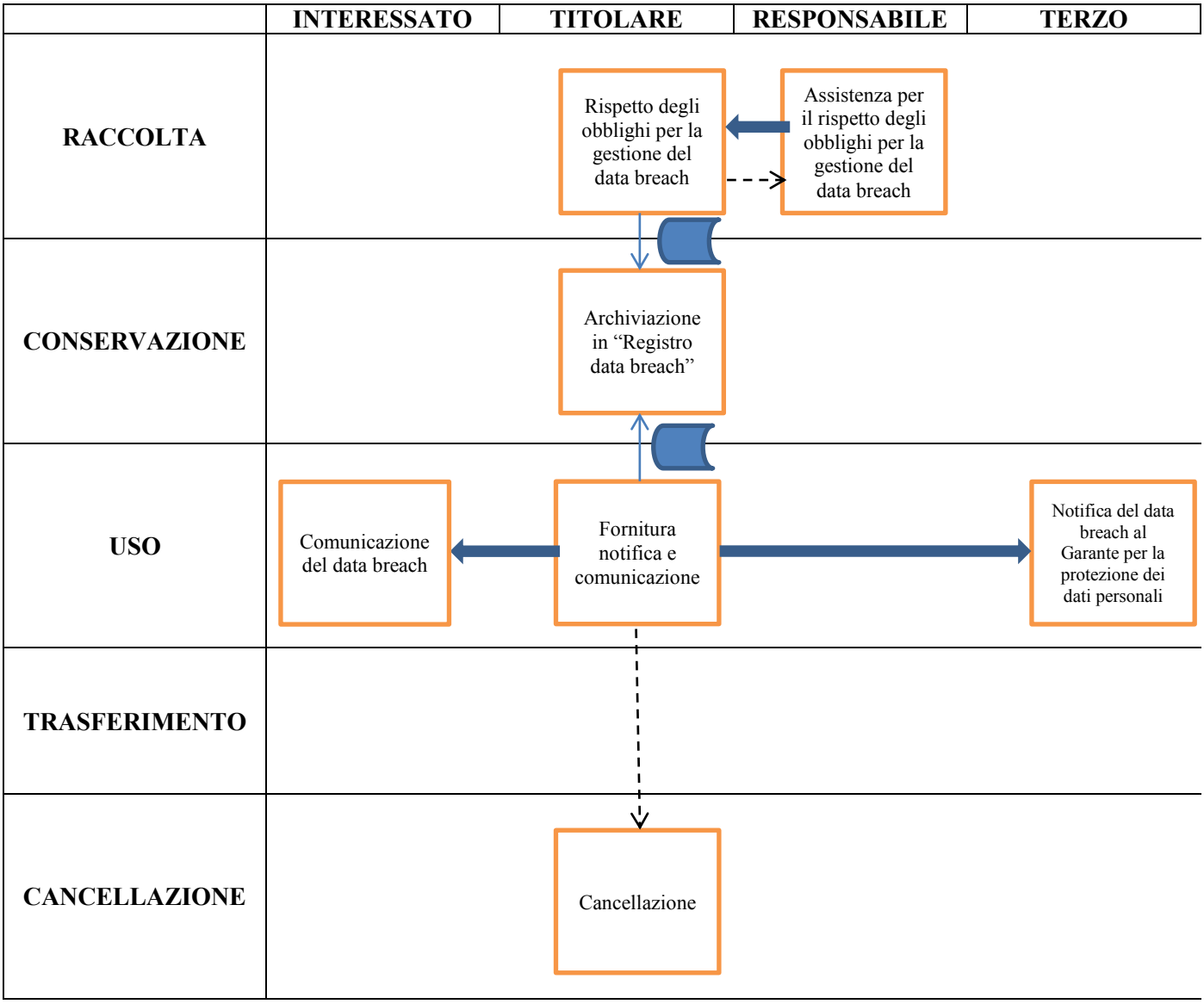
- RGPD:
  - Articolo 33 "*Notifica di una violazione dei dati personali all'autorità di controllo*";
  - Articolo 34 "*Comunicazione di una violazione dei dati personali all'interessato*".
- Pagina informativa dell'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI contenente link alla normativa e a documenti interpretativi, schede informative e pagine tematiche, tra cui quello alla "Compilazione della notifica on-line" (https://www.garanteprivacy.it/data-breach);

INTERNI:

- *Policy privacy* regolamento aziendale, delibera aziendale n. 403 del 29/07/2020;
- Codice di comportamento aziendale, delibera aziendale n. 1054 del 30/11/2022;
- Registro dei *Data breach*;

3. FLOW CHART

Fonte: *ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment*



Legenda

DATI PERSONALI

ISTRUZIONI

SERVIZIO

ARCHIVIAZIONE

DOCUMENTO

4. DESCRIZIONE DELLA PROCEDURA

L'**AUTORIZZATO** deve comunicare senza indugio l'accadimento di qualsiasi **DATA BREACH**, anche soltanto ipotetico, in modo da permettere al **TITOLARE** ASL 5 di notificare le violazioni, ritenute lesive dei diritti e delle libertà delle persone, all'**AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI** ed eventualmente di comunicarle agli **INTERESSATI**.

In caso di **DATA BREACH**, anche soltanto ipotetico, l'**AUTORIZZATO**, nel momento in cui ne viene a conoscenza anche indirettamente, è tenuto a segnalare l'accadimento senza indugio al coordinatore e/o all'incaricato di funzione organizzativa e/o al dirigente e/o al direttore/responsabile della struttura di afferenza.

Altresì, se la violazione di sicurezza è di tipo informatico deve essere segnalata immediatamente dall'**AUTORIZZATO** o da un responsabile della struttura di afferenza al Call Center S.I.A. – Sistema Informativo Aziendale (attivo dalle ore 07:00 alle ore 19:00, dal lunedì al venerdì e fino alle ore 13:00 il sabato: interno telefonico 2870, callcenterasl5@asl5.liguria.it) o al reperibile S.I.A. (attivo nei restanti orari notturni e festivi attraverso il centralino 0187 5331), che valuterà le attività da porre in essere al fine di annullare o di mitigare gli effetti della violazione. I dati da comunicare sono almeno i seguenti: luogo e momento di accadimento, durata e descrizione sommaria della violazione, compresa l'indicazione del *software*/applicativo/sistema digitale coinvolto nell'incidente di sicurezza.

In caso di trasmissione ad un soggetto non legittimato di una Pec/email contenente dati personali, l'**AUTORIZZATO** mittente chiede formalmente mediante lo stesso canale al destinatario non autorizzato di non utilizzarli e di cancellare fisicamente il messaggio.

In caso di violazione di sicurezza di tipo cartaceo, la segnalazione a un responsabile della struttura di afferenza deve essere accompagnata dall'adozione delle attività ritenute necessarie al fine di annullare o di mitigare gli effetti della violazione (es. mettere in sicurezza l'armadio, il locale etc. lasciato aperto e deprivato di un fascicolo etc. segnalando l'incidente agli altri **AUTORIZZATI** presenti).

La segnalazione effettuata dall'**AUTORIZZATO** a un responsabile della struttura di afferenza e, per gli aspetti informatici, al S.I.A., dopo le prime congiunte verifiche del caso, deve dare origine senza ingiustificato ritardo a una comunicazione al Responsabile della protezione dei dati (**RPD** interno telefonico 4300, privacy@asl5.liguria.it), contenente possibilmente tutte le seguenti informazioni necessarie alla compilazione del Registro dei *data breach* e all'eventuale notifica all'**AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**:

1) Luogo e momento di accadimento, durata e descrizione sommaria della violazione, compresa l'indicazione dell'archivio cartaceo e/o del *software*/applicativo/sistema digitale coinvolto nell'incidente;

2) Supposta causa della violazione (Azione intenzionale interna, Azione accidentale interna, Azione intenzionale esterna, Azione accidentale esterna, Sconosciuta);

3) Categorie di dati personali oggetto di violazione:
   (a) Dati anagrafici (es. nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale);
   (b) Dati di contatto (es. indirizzo postale o di posta elettronica, numero di telefono fisso o mobile);
   (c) Dati di accesso e di identificazione (es. *username*, *password*, *customer* ID);

(d) Dati relativi a condanne penali e ai reati;
(e) Dati relativi alla salute, alla vita sessuale, all'orientamento sessuale;
(f) Dati genetici;
(g) Dati biometrici;
(h) Appartenenza sindacale;
(i) Convinzioni religiose;
(j) Categorie ancora non determinate;

4) Volume (anche approssimativo) dei dati personali oggetto di violazione (es. numero di referti, numero di record di un database…);

5) Categorie di interessati coinvolti nella violazione (Dipendenti, Assistiti, Pazienti, Minori, Categorie ancora non determinate);

6) Numero (anche approssimativo) di interessati coinvolti nella violazione;

7) Descrizione delle eventuali misure adottate per porre rimedio alla violazione e mitigarne gli effetti negativi.

L'**AMMINISTRATORE DI SISTEMA** presenta ulteriori obblighi in caso di **DATA BREACH**. Rispetto alle soluzioni *on premises*, particolare attenzione dovrà essere posta a servizi di *cloud computing*, con riguardo all'ubicazione del server e alle modalità di gestione del registro dei log e degli eventi in connessione al rischio di accessi non autorizzati di terzi.

Pertanto, l'analisi di una violazione di sicurezza, in conseguenza della segnalazione al Call Center o al reperibile S.I.A. dell'incidente occorso, deve essere svolta dall'**AMMINISTRATORE DI SISTEMA** nella prospettiva della tutela dei diritti e delle libertà degli interessati.

Se la violazione di sicurezza viene rilevata autonomamente dall'**AMMINISTRATORE DI SISTEMA**, quest'ultimo deve procedere alla segnalazione immediata al proprio responsabile di struttura, di norma coincidente con la S.C. S.I.A., e di conseguenza alla comunicazione al Responsabile protezione dati (RPD), come sopra illustrato.

Anche il **RESPONSABILE (ESTERNO) DEL TRATTAMENTO** presenta peculiari obblighi in caso di **DATA BREACH**. L'assistenza al **TITOLARE** ASL 5, finalizzata al rispetto degli obblighi per la gestione di un **DATA BREACH,** è prevista all'interno del relativo Atto di nomina a responsabile del trattamento ex art. 28 **RGPD**.

In particolare, richiamata la vigente delibera aziendale n. 530/2021, ovvero le sue successive modifiche e integrazioni, avente a oggetto Completamento del "sistema privacy aziendale" con attivazione della "rete privacy", i direttori/responsabili di struttura, in ottemperanza alla sezione dell'Atto di nomina a responsabile (esterno) del trattamento dedicata a "*Notifica e comunicazione violazione dei dati (data breach), valutazione di impatto, consultazione preventiva*", devono vigilare affinché quest'ultimo comunichi al **TITOLARE** ASL 5 ogni evento di violazione di sicurezza.

Il **TITOLARE** ASL 5, a prescindere dalla notifica all'**AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI** e alla comunicazione agli **INTERESSATI**, deve comunque documentare nel Registro dei *data breach*, tenuto dal Responsabile della protezione dei dati (RPD), tutte le violazioni di sicurezza dei dati personali. La registrazione delle violazioni consente all'Autorità Garante di verificare il rispetto della normativa di settore.

Nei casi previsti, la notifica di una violazione di dati personali sarà trasmessa all'**AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI** a firma del **RPD** quale delegato del **TITOLARE** ASL 5 tramite la "Compilazione della notifica on-line" (https://www.garanteprivacy.it/data-breach).

Nei casi previsti, la comunicazione di una violazione di dati personali sarà trasmessa all'**INTERESSATO/A** dal **TITOLARE** ASL 5 a firma del Direttore Generale.

La cancellazione della documentazione inerente la gestione di una violazione di dati personali avviene a cura del Responsabile della protezione dei dati (**RPD**) secondo le tempistiche stabilite nel vigente massimario aziendale di scarto.

Fase	Descrizione	Responsabile	Input	Output
1	RACCOLTA DATI	AUTORIZZATO (DIPENDENTE, CONVENZIONATO, ALTRO OPERATORE)	ACCADIMENTO DI DATA BREACH	1) SEGNALAZIONE AL PROPRIO RESPONSABILE DI STRUTTURA (COORDINATORE, I.F.O., DIRIGENTE, DIRETTORE/RESPONSABILE) 2) In caso di violazione di tipo informatico, SEGNALAZIONE ALLA SC SIA – CALL CENTER 3) SEGNALAZIONE AL RESPONSABILE PROTEZIONE DATI (RPD)
2	CONSERVAZIONE	RESPONSABILE PROTEZIONE DATI (RPD)	SEGNALAZIONE DI DATA BREACH	REGISTRAZIONE DELLE INFORMAZIONI RELATIVE AL DATA BREACH
3	USO	RESPONSABILE PROTEZIONE DATI (RPD)	SEGNALAZIONE DI DATA BREACH	NEI CASI PREVISTI, NOTIFICA DEL DATA BREACH ALL'AUTORITÀ GARANTE
4	USO	TITOLARE DEL TRATTAMENTO	NOTIFICA DEL DATA BREACH ALL'AUTORITÀ GARANTE	NEI CASI PREVISTI, COMUNICAZIONE ALL'INTERESSATO

Fase	Descrizione	Responsabile	Input	Output
5	CANCELLAZIONE	RESPONSABILE PROTEZIONE DATI (RPD)	REGISTRAZIONE DELLE INFORMAZIONI RELATIVE AL DATA BREACH	CANCELLAZIONE DELLA DOCUMENTAZIONE SECONDO IL MASSIMARIO DI SCARTO AZIENDALE

INFORMAZIONI AGGIUNTIVE EX ART. 13 RGPD

Le informazioni sul trattamento eseguito dal **TITOLARE** ASL 5 sono disponibili in forma completa e trasparente nell'Informativa Generale resa ai sensi degli artt. 13 e 14 RGPD, disponibile su https://www.asl5.liguria.it/Portals/0/Privacy/InformativaGenerale.pdf (assistiti, pazienti e utenti) e https://www.asl5.liguria.it/Portals/0/Privacy/informazionirapportolc.pdf (dipendenti, convenzionati e altri operatori del sistema *privacy* aziendale), informazioni che qui devono intendersi integralmente applicabili, comprese quelle relative ai termini di conservazione dei dati.

Altresì, alla pagina *web* https://www.asl5.liguria.it/privacy.aspx sono disponibili i dati di contatto sia del **TITOLARE** del trattamento ASL 5 sia del Responsabile aziendale della protezione dei dati personali (**RPD**). Alla predetta pagina *web* è disponibile la presente procedura per la Gestione di una violazione di dati personali.

Il trattamento dei dati personali inerente la Gestione di un **DATA BREACH** è necessario per le finalità connesse all'applicazione del **RGPD** ed è lecito in quanto necessario per adempiere un obbligo legale al quale è soggetto il **TITOLARE** del trattamento (artt. 6, par. 1, lett. c), **RGPD**)..

IL TITOLARE DEL TRATTAMENTO
AZIENDA SOCIOSANITARIA LIGURE 5