TITOLARE DEL TRATTAMENTO

Asl5

Sistema Sanitario Regione Liguria

Ufficio del RESPONSABILE PROTEZIONE DATI
RPD: Vattovani Alessandro
TEL: 0187 534300
Mail: privacy@asl5.liguria.it
PEC: dpo@pec.asl5.liguria.it
WEB: http://www.asl5.liguria.it/privacy.aspx
http://portale.asl5.local/it-it/privacy.aspx

Istruzione operativa

VIOLAZIONE DI DATI PERSONALI: GESTIONE DEL *DATA BREACH*

Artt. 33 e 34 Regolamento (UE) 2016/679

COS'È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)?

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 trattati.

Una **violazione di sicurezza** può compromettere la **confidenzialità**, l'**integrità** o la **disponibilità** 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 la confidenzialità dei dati personali, l'OPERATORE "*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*". L'OPERATORE "*non intrattiene rapporti con i mezzi d'informazione in merito alle attività istituzionali*". L'OPERATORE "*informa la Direzione aziendale qualora sia destinatario di richieste da parte di organi di informazione per avere istruzioni sul comportamento da tenere nel caso specifico*" (*cfr.* vigente Codice di comportamento aziendale).

SCOPO DELL'ISTRUZIONE OPERATIVA

Disegnare un flusso per la gestione delle **violazioni di sicurezza** occorse in **ASL 5** e rilevate dagli **OPERATORI, interni ed esterni, attivi in ASL 5 (**qualunque sia il rapporto giuridico), afferenti sia al comparto sia alla dirigenza, incaricati del trattamento di dati personali.

È di fondamentale importanza che tutto il **Sistema *privacy* aziendale** si attivi senza indugio nell'eventualità in cui si presentino **violazioni di sicurezza** concrete, potenziali o anche sospette di dati personali, in modo da poter comunicare, nei casi previsti, la violazione all'Autorità Garante (entro 72 ore) e agli Interessati (senza ingiustificato ritardo), ciò al fine di evitare rischi per i diritti e le libertà delle persone, nonché possibili danni economici all'Azienda.

DEFINIZIONI

TITOLARE: ASL 5 che determina finalità e mezzi del trattamento di dati personali degli Interessati;

INTERESSATO: **LA PERSONA** (fisica) alla quale si riferiscono i dati trattati da **ASL 5**;

AUTORIZZATO: **L'OPERATORE, INTERNO O ESTERNO, ATTIVO IN ASL 5 (**qualunque sia il rapporto giuridico), afferente al comparto o alla dirigenza, incaricato del trattamento di dati personali;

Ufficio del RESPONSABILE PROTEZIONE DATI
RPD: Vattovani Alessandro
TEL: 0187 534300
Mail: privacy@asl5.liguria.it
PEC: dpo@pec.asl5.liguria.it
WEB: http://www.asl5.liguria.it/privacy.aspx
http://portale.asl5.local/it-it/privacy.aspx

AMMINISTRATORE DI SISTEMA: L'OPERATORE, INTERNO O ESTERNO, ATTIVO IN ASL 5 (qualunque sia il rapporto giuridico), afferente al comparto o alla dirigenza, 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;

RESPONSABILE (ESTERNO) DEL TRATTAMENTO: il Fornitore, *lato sensu* considerato, di beni, servizi, lavori che effettua un trattamento di dati personali degli Interessati per conto del Titolare **ASL 5**;

DATO PERSONALE: qualsiasi informazione riguardante una persona fisica identificata o identificabile;

I dati personali sono di diverso tipo: alcuni sono di categoria particolare (dati sensibili), altri di tipo giudiziario, altri ancora "comuni" (ulteriormente classificabili in dati anagrafici, di contatto, di accesso …);

- **DATI DI CATEGORIA PARTICOLARE**: *dati genetici, 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, dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale.*

L'elencazione dei **dati di categoria particolare** è tassativa, non ampliabile. Si evidenziano quelli principalmente trattati in un'azienda sanitaria:

  - **DATI GENETICI**: *dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione*;
  - **DATI BIOMETRICI**: *i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*;
  - **DATI RELATIVI ALLA SALUTE**: *i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*;

- **DATI GIUDIZIARI**: dati personali relativi a condanne penali e reati;

- **DATI "COMUNI"**: tutti gli altri dati, ovverosia quelli che permettono l'identificazione diretta dell'interessato, come il nominativo e le immagini, e quelli che ne permettono l'identificazione indiretta, come il codice fiscale, il codice assistito, la targa del veicolo, la residenza, il domicilio, il numero di telefono, l'indirizzo e-mail/pec, l'indirizzo IP, il reddito, il livello di istruzione, la geolocalizzazione etc.;

- **TRATTAMENTO DI DATI PERSONALI**: *qualsiasi operazione, compiuta con l'ausilio di processi automatizzati* (dati personali digitali) *e/o senza l'ausilio di processi automatizzati* (dati personali cartacei)*, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione di dati personali*.

COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI?

L'**OPERATORE** deve comunicare senza indugio l'accadimento di **QUALUNQUE VIOLAZIONE DI SICUREZZA** (anche soltanto ipotetica) in modo da permettere ad **ASL 5** di notificare le violazioni, ritenute lesive dei diritti e delle libertà delle persone, al Garante per la protezione dei dati personali e agli Interessati.

ASL 5, a prescindere dalla notifica al Garante, 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.

QUALI GLI OBBLIGHI DELL'OPERATORE?

In caso di violazione di dati personali (anche soltanto ipotetica), l'**OPERATORE**, nel momento in cui ne viene a conoscenza, anche indirettamente, è tenuto a segnalarla **immediatamente** (in caso di violazione di sicurezza di tipo informatico) ovvero **entro 12 ore** (in caso di violazione di sicurezza di tipo cartaceo) al Capo-turno e/o al Coordinatore e/o alla Posizione organizzativa e/o al Dirigente e/o al Referente *privacy* e/o al Direttore/Responsabile della Struttura di afferenza.

Altresì, la **violazione di sicurezza di tipo informatico** deve essere segnalata **immediatamente** dall'**OPERATORE** o dal suo responsabile al *Call Center* S.I.A. – Sistema Informativo Aziendale (attivo dalle ore 07:00 alle ore 19:00, dal lunedì al sabato: int. 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 almeno di ridurre gli effetti della violazione. I dati da comunicare sono, quanto meno, quelli di cui al successivo punto 1: luogo e momento di accadimento, durata e descrizione sommaria della violazione, compresa l'indicazione del *software*/applicativo/sistema digitale coinvolto nell'incidente. In caso di trasmissione ad un soggetto non legittimato di una Pec/*email* contenente dati personali, l'**OPERATORE** mittente chiede formalmente al destinatario non autorizzato, mediante lo stesso canale, di non utilizzarli e di cancellare fisicamente il messaggio.

Se, in caso di **violazione di sicurezza di tipo cartaceo**, la segnalazione al proprio responsabile avviene successivamente, ma entro 12 ore, dall'accadimento del *data breach*, ciò non esime l'**OPERATORE** dal porre in essere immediatamente le attività ritenute necessarie al fine di annullare o almeno ridurre gli effetti della violazione (es. mettere in sicurezza l'armadio, il locale etc. lasciato aperto e deprivato di un fascicolo segnalando l'incidente ai colleghi presenti).

La segnalazione effettuata dall'**OPERATORE** ad almeno uno dei propri responsabili e, se del caso, 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 (R.P.D. privacy@asl5.liguria.it), contenente possibilmente tutte le seguenti informazioni necessarie alla compilazione del Registro dei *data breach* e all' eventuale notifica al Garante:

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, Altro da specificare);***
3. ***Categorie di dati personali oggetto di violazione [Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...); Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile); Dati di accesso e di identificazione (username, password, customer ID, altro…); Dati relativi a condanne penali e ai reati; Dati relativi alla salute; Dati genetici; Dati biometrici; Categorie ancora non determinate; Altro da specificare];***
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, Altro da specificare);***
6. ***Numero (anche approssimativo) di interessati coinvolti nella violazione;***
7. **[CON PARTICOLARE ATTENZIONE ALLA]** ***Descrizione delle eventuali misure adottate o che si ritiene possano essere adottate in futuro per porre rimedio alla violazione e attenuarne se possibile gli effetti negativi.***

QUALI GLI OBBLIGHI DELL'AMMINISTRATORE DI SISTEMA?

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., deve essere svolta dall'**AMMINISTRATORE DI SISTEMA** anche mediante l'effettuazione di una vera e propria D.P.I.A. (*data protection impact assessment*) dell'incidente occorso, nella prospettiva della tutela dei diritti e delle libertà degli interessati.

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

QUALI GLI OBBLIGHI DEL RESPONSABILE (ESTERNO) DEL TRATTAMENTO?

Analoghi obblighi di segnalazione sono previsti all'interno dell'Atto di designazione del Responsabile (esterno) del trattamento ex art. 28 RGPD (e degli Accordi di contitolarità ex art. 26 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 coadiuvati dai loro Referenti privacy, in ottemperanza all'articolo dell'Atto di designazione del Responsabile (esterno) del trattamento dedicato 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.

* * *

La presente Istruzione Operativa:

- è pubblicata, a cura del Responsabile della protezione dei dati, alla pagina "*Privacy*" del sito *internet* e *intranet* aziendale;

- è trasmessa con *email* circolare, a cura del Responsabile della protezione dei dati, a tutti gli *account* aziendali;

- è resa disponibile in copia cartacea, a cura di ogni Direttore/Responsabile di Struttura aziendale, presso un locale ad accesso comune a disposizione di tutti gli **OPERATORI, interni ed esterni, attivi in ASL 5** (qualunque sia il rapporto giuridico), afferenti sia al comparto sia alla dirigenza, incaricati del trattamento di dati personali.

IL TITOLARE DEL TRATTAMENTO

AZIENDA SOCIOSANITARIA LIGURE 5