ASLGallura
Azienda socio-sanitaria locale

Azienda Socio Sanitaria Locale n. 2 Gallura
Dipartimento Area Amministrativa
SC Area Affari Generali, Legali
e Capitale Umano

Procedura data breach

Linee guida per la gestione delle violazioni di dati personali e la loro eventuale comunicazione all'Autorità e ai soggetti interessati

DIREZIONE ASL 2 GALLURA
0789 552200
Via Bazzoni Sircana 2 – 2 A
CAP 07026 Olbia
P.IVA: 02891650901
0789 552305-374
protocollo@pec.aslgallura.it
www.aslgallura.it

SC Area Affari Generali, Legali e Capitale Umano
0789 / 552360
Via Bazzoni Sircana 2-2A
07026 Olbia
sc.aaggll.capum@aslgallura.it

Indice

Sommario

1. Premessa

Secondo quanto previsto dall'art. 4 («Definizioni») del Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito, "GDPR" o "Regolamento"), per violazione dei dati personali si intende «*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*».

In tale contesto, l'art. 33 del Regolamento sancisce l'obbligo per il titolare del trattamento di notificare tempestivamente l'avvenuta violazione dei dati personali (c.d. "*Data Breach*") all'autorità di controllo e, in casi determinati e con specifiche modalità, di procedere alla comunicazione direttamente agli interessati.

L'obiettivo del presente documento è disciplinare il processo di gestione delle violazioni di dati personali, funzionale a definire i principi generali, i ruoli, le responsabilità e le attività da effettuare qualora si verifichi un incidente di sicurezza che comporti la violazione di dati personali trattati a qualunque titolo dall'Azienda e dalle sue articolazioni.

Oggi, il Cyber Risk (o Rischio informatico) ha raggiunto livelli altissimi, aggravato peraltro dall'utilizzo dell'AI. E' un fenomeno che interessa tutti, Pubbliche Amministrazioni incluse e può tradursi in varie forme.

Tra gli attacchi informatici più comuni:

- **Malware**: qualsiasi programma informatico in grado di prendere il controllo (totale o parziale) di un dispositivo fino raccogliere informazioni private, creare malfunzionamenti, criptare i dati o addirittura bloccarne l'accesso. Si tratta di fenomeni prevedibili, ma non troppo: spesso possono arrivare attraverso una semplice mail, un allegato, un link o un banner pubblicitario, o una app da installare, ma anche con siti web creati apposta per infettare il sistema. A volte può capitare che il malware obblighi al pagamento di un riscatto per accedere di nuovo al dispositivo; in questo caso si parla di **ransomware** (da "ransom", "riscatto" in inglese).
- **Phishing**: truffe informatiche mirate a estorcere informazioni e dati personali alle vittime (per esempio password o qualsiasi altro codice di accesso) "mascherandosi" da ente affidabile o da soggetto autorizzato. È il caso, molto frequente, delle finte e-mail contraffatte di banche, Poste, assicurazioni e quant'altro.

La presente procedura si applica a tutte le violazioni di dati personali (come di seguito meglio identificate) riscontrate all'interno dell'Azienda e spiega la sua efficacia nei confronti di tutti i dipendenti della stessa.

2. Definizione di una violazione dei dati personali

Con il termine "*violazione dei dati personali*" (in inglese "*data breach*") si intende un evento (violazione di sicurezza) che può comportare, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso a informazioni qualificate dal Regolamento come dati personali trasmessi, memorizzati o elaborati per mezzo di sistemi informatici o di altra natura.
Richiamate le disposizioni di cui alle Linee guida EDPB n. 9/2022 del 27/03/2023 sulla notifica delle violazioni dei dati personali ai sensi del regolamento generale sulla protezione dei dati (GDPR), la natura della violazione può essere classificata in base ai seguenti principi di sicurezza delle informazioni:

- "**perdita di confidenzialità**": diffusione, accesso non autorizzato o accidentale;
- "**perdita di integrità**": modifica non autorizzata o accidentale;
- "**perdita di disponibilità**": impossibilità di accesso, perdita, distruzione non autorizzata o accidentale.

Vengono forniti alcuni esempi significativi di data breach che possono essere di utilità per inquadrare il contesto

Perdita di un dispositivo non protetto da cifratura	Anche il semplice smarrimento di uno smartphone può costituire una valida ragione di un data breach nel caso in cui contenga Dati personali in ragione della loro quantità e qualità, e non sia stato opportunamente cifrato. Può potenzialmente costituire perdita di riservatezza e di disponibilità, qualora non esistano altre copie del dato.
Invio errato di una e mail contenente un archivio con dati identificativi e di contatti di pazienti	Un esempio potenziale di perdita di confidenzialità del dato è quando un Dato personale viene inviato per errore ad un terzo non autorizzato.
Cancellazione o modifica inavvertita di un archivio (es: di un foglio di calcolo contenente) dati personali in grande quantità senza che sia presente un backup o una copia di sicurezza	Un esempio di perdita di disponibilità (nel caso di cancellazione) o di integrità (modifica inavvertita) del dato si verifica quando un Dato personale non è adeguatamente protetto da modifiche e cancellazioni e non è presente una copia di sicurezza aggiornata con regolarità. In pratica quando si fa uso di strumenti non centralizzati e non adeguatamente protetti ci si espone al rischio di perdita di dati o di introduzione di dati errati.

2.1 Tipologie di Data Breach

Di seguito si riportano le principali possibili violazioni di dati personali identificate:

- furto o smarrimento di beni dell'Azienda, connesso ad un comportamento negligente di dipendenti/collaboratori, che può verificarsi nel caso in cui venga meno il controllo degli strumenti utilizzati per elaborare i dati personali (Server, PC/laptop, smartphone, device per l'archiviazione di dati esterni);
- accesso illegale da parte di soggetti terzi, ossia accesso abusivo da parte di terzi, non autorizzati, ai sistemi informatici, ad esempio, mediante:
    - un attacco *ransomware*, mirato al furto di documenti. Questo tipo di attacco di solito può essere classificato come violazione della disponibilità dei dati personali, ma spesso potrebbe verificarsi anche una violazione della riservatezza degli stessi;
    - attacchi *injection* (*SQL injection, path traversal*). Tali attacchi mirano a copiare e abusare dei dati personali. Si tratta principalmente di violazioni della riservatezza, ma spesso potrebbe verificarsi anche una violazione dell'integrità degli stessi;
    - attacchi *phishing*, ossia truffe informatiche effettuate inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati, motivando tale richiesta con ragioni di ordine tecnico. Tali attacchi sono classificati come violazioni della riservatezza dei dati personali;
- errore accidentale da parte di uno dei soggetti che trattano dati personali (i.e. invio di una mail contenente dati personali ad un destinatario errato);
- furto di informazioni, può verificarsi nel caso in cui un dipendente (o ex dipendente) sfrutti la propria conoscenza o le proprie autorizzazioni per sottrarre dolosamente dati/informazioni di carattere personale;
- vigilanza/adozione di misure di sicurezza, qualora, a causa di un'erronea valutazione sul livello di criticità dei dati e/o informazioni ministeriali, non siano state poste in essere le necessarie precauzioni volte alla salvaguardia dei dati medesimi, che sono stati perduti.

3. Ruoli e responsabilità

Coerentemente con il "*Regolamento aziendale in materia di Privacy",* approvato con Delibera del Direttore Generale n. 474 del 10/06/2024, si riportano di seguito i ruoli e le responsabilità di ciascuna figura coinvolta nel processo di gestione e segnalazione delle violazioni:

- su delega del Direttore Generale, il **Direttore SC Area Affari Generali, Legali e Capitale Umano**, all'interno della quale è incardinato l'Ufficio Privacy aziendale: dopo aver valutato la portata e il livello di rischio della avvenuta violazione di dati personali, si occupa di individuare e adottare possibili misure di rimedio sentiti, ove necessario, i competenti Servizi Informativi istituiti presso il Dipartimento Sanità Digitale e Innovazione Tecnologica di ARES Sardegna e, ove necessario, di notificare la violazione all'autorità di controllo competente entro 72 ore dal momento in cui ne è venuto a conoscenza, salvo che si riveli improbabile che la violazione medesima possa presentare un rischio per i diritti e le libertà delle persone fisiche. Comunica la violazione agli interessati, anche avvalendosi dei Servizi Informativi di cui sopra, qualora la stessa sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Programma e attua attività di verifiche periodiche volte a garantire l'efficacia delle procedure e degli strumenti di risposta agli incidenti relativi alle violazioni di dati personali;
- **Responsabile della protezione dei dati**: funge da punto di contatto tra il titolare, il Garante e gli interessati; nell'ambito della gestione degli incidenti, congiuntamente all'Ufficio Privacy aziendale raccoglie tutte le possibili violazioni di dati personali e individua il Dirigente designato che sarà competente per la gestione della eventuale violazione. Avvalendosi della collaborazione dell'Ufficio Privacy aziendale, svolge funzioni di supporto al Titolare del Trattamento oltrechè al Direttore SC Area Affari Generali, Legali e Capitale Umano. Il RPD ha una funzione di consulenza e supporto, non potendosi in alcun caso sostituire al soggetto che esercita le funzioni di titolare nell'assolvimento dei compiti e nelle decisioni che spettano a quest'ultimo, salva diversa disposizione di legge;
- **Ufficio Privacy aziendale**: istituito all'interno della SC Area Affari Generali, Legali e Capitale Umano, svolge attività di supporto e consulenza all'Azienda per le questioni relative alla tutela dei dati personali trattati e rappresenta il punto di contatto con il RPD. In tale veste, le risorse umane assegnate all'Ufficio si occupano di:
    - raccogliere le segnalazioni di potenziali data breach, ricevute dal RPD, ovvero da qualsiasi altra fonte esterna o interna, e di trasmettere immediatamente le stesse al responsabile interno coinvolto;
    - coadiuvare i Direttori di Struttura nella valutazione della segnalazione;

- tenere e aggiornare il **registro delle violazioni** (**allegato 1**), secondo le istruzioni illustrate nel prosieguo;
- supportare il RPD anche attraverso la messa a disposizione in suo favore di tutti gli elementi valutativi necessari l'espletamento dei suoi compiti.

- **Direttore di Struttura** (Direttori di Dipartimento, di Struttura Complessa, di Struttura Semplice o Semplice Dipartimentale, sia quelli appartenenti all'Area della Dirigenza Sanità che quelli all'Area Funzioni Locali): in qualità di Dirigente designato allo svolgimento di specifici compiti e funzioni connessi al trattamento, svolge le seguenti attività:
  - adotta le misure di sicurezza tecnico/organizzative previste dalla normativa interna;
  - coordina le attività degli autorizzati al trattamento e si interfaccia con gli Amministratori di Sistema;
  - ove ritenga che l'incidente occorso possa aver comportato una violazione dei dati personali, informa senza ritardo il Direttore della SC Area Affari Generali, Legali e Capitale Umano;
  - fornisce, con l'ausilio degli autorizzati al trattamento, degli Amministratori di Sistema, e dell'Ufficio Privacy aziendale, elementi utili per l'eventuale predisposizione delle comunicazioni da trasmettere al Garante privacy e agli interessati.
- **Autorizzati**: soggetti preposti, sotto l'autorità diretta del Titolare, ad una o più attività di trattamento che coadiuvano il Direttore di Struttura all'interno della quale risultino assegnati, svolgendo le seguenti attività:
  - comunicano eventuali violazioni di dati personali di cui sono a conoscenza mediante l'invio di una comunicazione da inviare alla mail appositamente istituita: databreach@aslgallura.it;
  - forniscono supporto in fase identificazione dell'incidente, comunicando ai Direttori di Struttura di riferimento, le informazioni utili per la classificazione delle violazioni verificatesi.
- **Amministratori di Sistema** (di seguito anche "AdS"): premesso che, ai sensi della Legge regionale n. 24/2020, Ares Sardegna è il soggetto responsabile della gestione centralizzata delle infrastrutture di tecnologia informatica, connettività, sistemi informativi e flussi dati in un'ottica di omogeneizzazione e sviluppo del sistema ICT, l'Azienda non ha alcuna autonomia nella gestione operativa dei sistemi informativi e nella definizione delle misure di sicurezza di cui all'art. 32 del Regolamento UE 2016/679. Per questo motivo, al verificarsi di un evento avverso, causato da o che comprometta i sistemi informativi aziendali, ASL Gallura per il tramite dell'Ufficio Privacy provvederà a contattare immediatamente, senza indugio, i competenti Servizi Informativi istituiti presso il Dipartimento Sanità Digitale e Innovazione Tecnologica di ARES Sardegna per richiedere tempestiva assistenza al fine di mitigare le conseguenze dell'evento avverso e rimuovere le cause che l'hanno determinato;

tali soggetti che, in qualità di preposti alle attività di gestione e manutenzione dei sistemi informatici, svolgono in linea generale le seguenti attività:

- monitorano i sistemi di sicurezza;
- comunicano in caso di violazione tutte le informazioni necessarie alla sua comprensione e le trasmettono all'Asl Gallura;
- comunicano le eventuali azioni poste in essere per la gestione della violazione all'Ufficio Privacy aziendale e al RPD;
- monitorano nel continuo le attività necessarie a prevenire eventuali violazioni/ e le attività che rilevino le eventuali non conformità delle misure di sicurezza;
- comunicano all'Ufficio Privacy aziendale e al RPD eventuali situazioni che potrebbero comportare violazioni di dati personali;
- raccolgono le informazioni per quanto di competenza, necessarie a formulare compiutamente le comunicazioni verso il Garante /Interessato.

4. Riferimenti

Di seguito l'elenco dei **documenti** che costituiscono il **riferimento** per le presenti linee guida:

- Regolamento UE n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla protezione dei dati);
- D.Lgs. n. 196/03 Codice in materia di protezione dei dati personali e successive modifiche e integrazioni;
- Linee guida EDPB n. 9/2022 del 27/03/2023 sulla notifica delle violazioni dei dati personali ai sensi del regolamento generale sulla protezione dei dati (GDPR);
- Provvedimento n. 209 del Garante del 27 maggio 2021 sulla Procedura telematica per la notifica di violazioni di dati personali (*data breach*).
- *"Regolamento aziendale in materia di Privacy",* approvato con Delibera del Direttore Generale n. 474 del 10/06/2024.

5. Procedura di data breach

La procedura di *data breach* adottata dall'ASL Gallura è articolata nelle seguenti fasi:

1) IDENTIFICAZIONE
2) SEGNALAZIONE
3) VALUTAZIONE
4) NOTIFICA
5) REGISTRAZIONE
6) PIANO DI RIMEDIO

PROCESSO DI VIOLAZIONE DEI DATI PERSONALI – FASI 1, 2 E 3			
	IDENTIFICAZIONE	SEGNALAZIONE	VALUTAZIONE

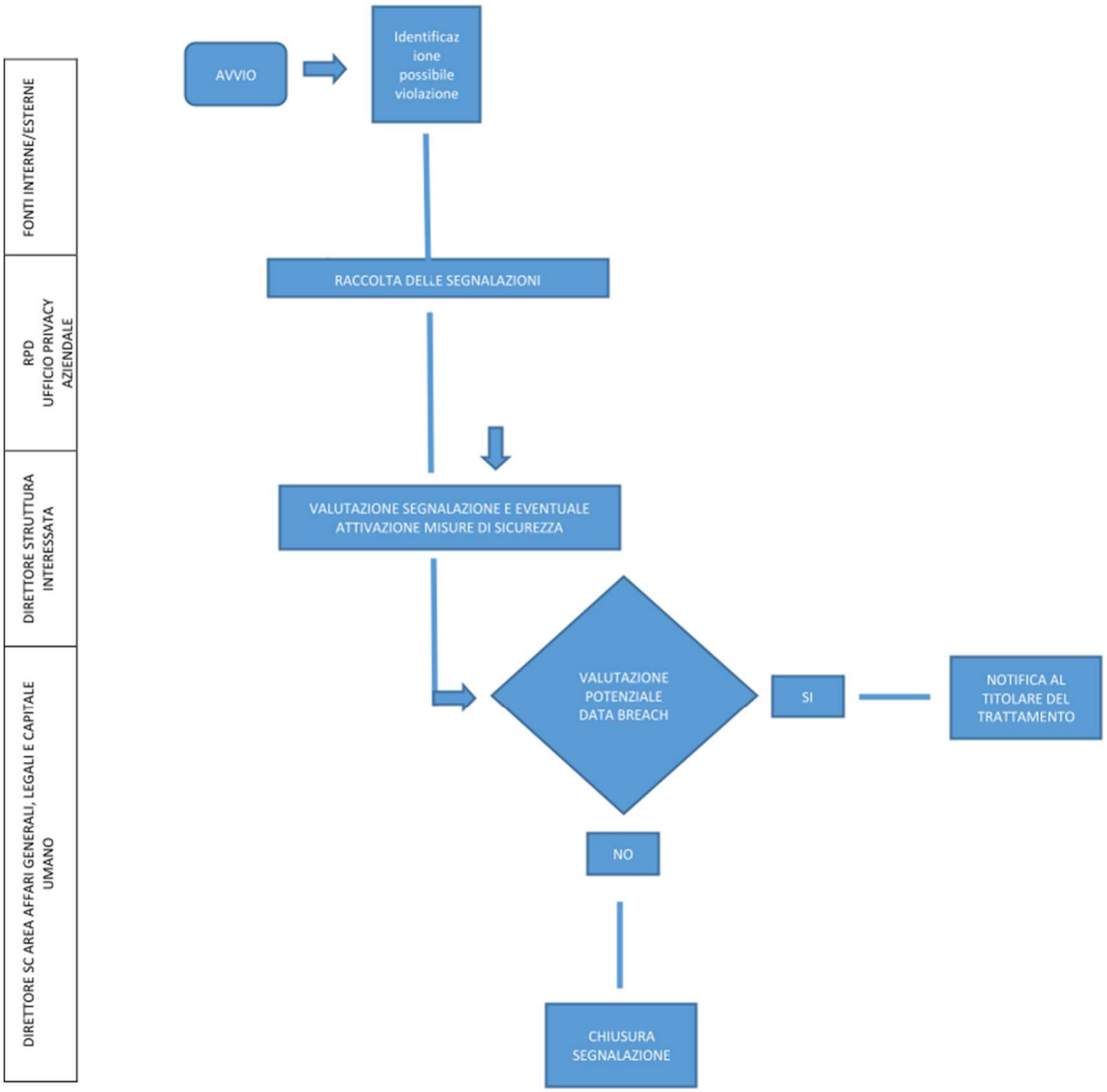

Figura 1 – Procedura di data breach fasi 1-2-3

PROCESSO DI VIOLAZIONE DEI DATI PERSONALI – FASI 4, 5 E 6			
	NOTIFICA	REGISTRAZIONE	PIANO DI RIMEDIO

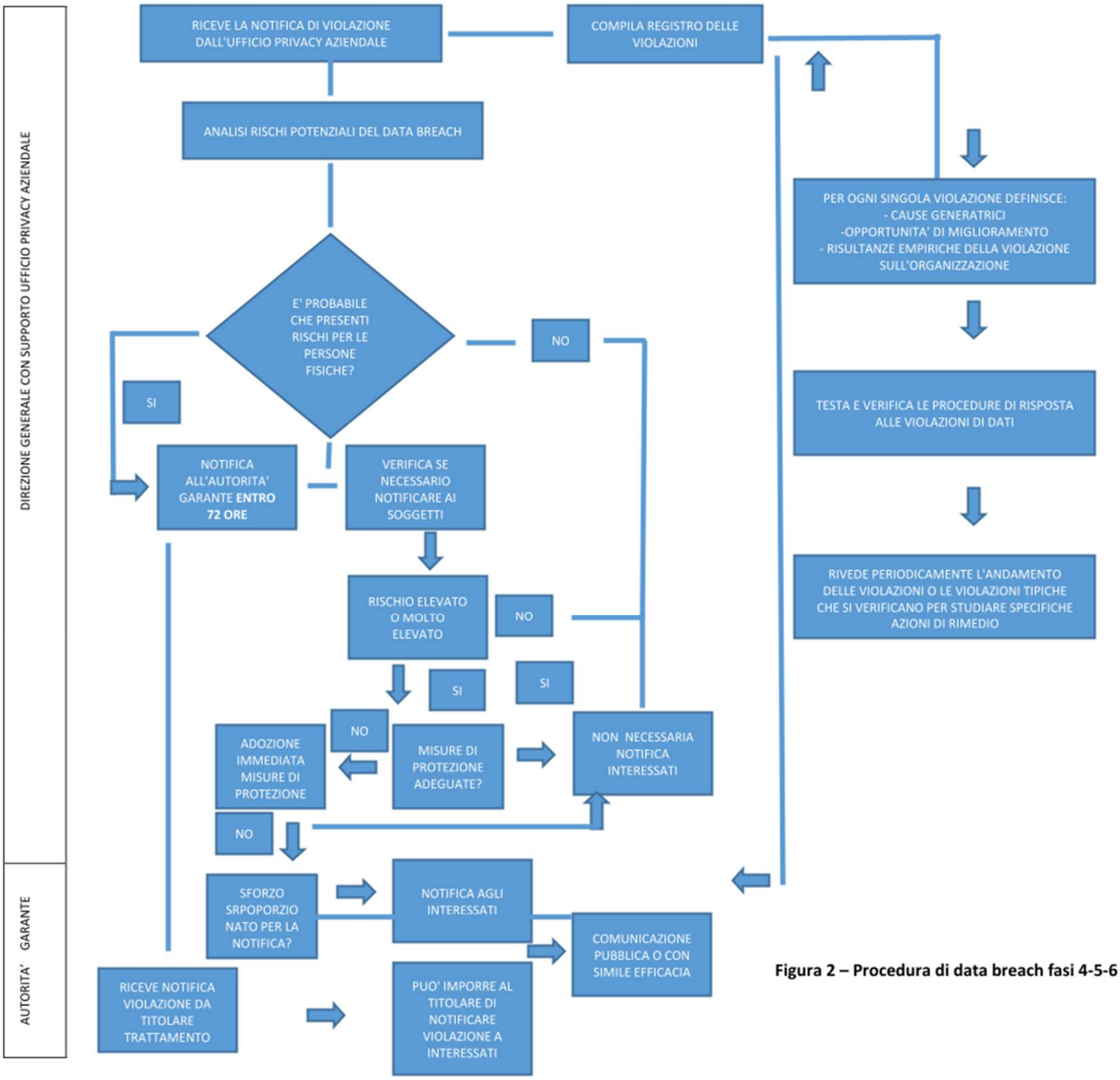

Figura 2 – Procedura di data breach fasi 4-5-6

6. Identificazione di un potenziale data breach

La fase di identificazione di una violazione di dati personali ha l'obiettivo di rilevare un potenziale *data breach* derivante dalla perdita, divulgazione non autorizzata, trattamento illecito e/o perdita di disponibilità di dati personali di cui ASL Gallura è titolare.
Tutte le possibili violazioni dei dati personali devono essere identificate e indirizzate tempestivamente all'Ufficio Privacy aziendale, afferente alla SC Area Affari Generali, Legali e Capitale Umano e al Responsabile della protezione dei dati unicamente mediante il seguente indirizzo mail: databreach@aslgallura.it.
Il Direttore della SC Area Affari Generali, Legali e Capitale Umano, avvalendosi dell'Ufficio Privacy aziendale, una volta ricevuta la segnalazione provvede ad inoltrarla tempestivamente al Protocollo Aziendale, che a sua volta si farà carico di assegnarla, **nella medesima giornata di ricezione** ai seguenti destinatari:

- Responsabile della Protezione Dati;
- Direzione Generale;
- Servizi Informativi istituiti presso il Dipartimento Sanità Digitale e Innovazione Tecnologica di ARES Sardegna;
- Sc Area Tecnologia e Transizione Digitale.

Le segnalazioni possono provenire da fonti interne e fonti esterne all'ASL, quali:

- Strumenti informatici di monitoraggio di eventi di sicurezza o attraverso misure tecniche di sicurezza finalizzate alla protezione dei sistemi informativi;
- Dipendenti/autorizzati al trattamento;
- Cittadini;
- Fornitori e terze parti;
- Autorità di vigilanza;
- Forze di Polizia;
- Media (es. stampa, telegiornali, agenzie di informazione multimediale, ecc.);

Ogni soggetto che presta la propria attività a favore dell'ASL Gallura, che venga a conoscenza o sospetti che sia avvenuta una violazione di dati personali, deve darne immediata comunicazione tramite invio di una mail all'indirizzo ***databreach@aslgallura.it***.
La comunicazione deve contenere un'indicazione chiara dell'evento verificatosi, delle caratteristiche dei dati personali coinvolti e, ove possibile, dell'unità organizzativa interessata dalla violazione, come da scheda segnalazione - **allegato 2** alla presente.

Il competente Ufficio Privacy aziendale, una volta ricevuta la comunicazione sul potenziale *data breach*, informa, senza ritardo, il Titolare del trattamento, legalmente rappresentato dal Direttore Generale, competente per la gestione della eventuale violazione e la trasmette, come detto, al Responsabile della Protezione Dati, ai Servizi Informativi istituiti presso il Dipartimento Sanità Digitale e Innovazione Tecnologica di ARES Sardegna nonchè alla Sc Area Tecnologia e Transizione Digitale dell'Asl Gallura.
Ai fini istruttori, l'Ufficio Privacy inoltra la comunicazione pervenuta al Responsabile o ai Responsabili interni presso la/le cui Struttura/e la violazione si sia verificata, al fine di acquisire tutte le informazioni necessarie alla gestione della stessa, mediante dettagliata relazione che la/le stessa/e sono tenute a rendere **entro 24 ore dall'avvenuta ricezione della comunicazione di violazione.**
Qualora la presunta violazione inerisca a dati personali trattati da un responsabile del trattamento, sarà dovere dello stesso rilevarla e darne comunicazione all'ASL Gallura, per il tramite del competente Ufficio Privacy aziendale, mediante comunicazione mail all'indirizzo ***databreach@aslgallura.it***.

7. Esecuzione dei riscontri interni

Il Direttore della SC Area Affari Generali, Legali e Capitale Umano, avvalendosi dell'Ufficio Privacy aziendale, ricevuta la comunicazione della presunta violazione di dati personali, effettua le verifiche necessarie volte a vagliarne l'attendibilità. Al fine di condurre una valutazione sulla presunta violazione, l'Ufficio Privacy potrà avvalersi dell'ausilio dello strumento di autovalutazione messo a disposizione dei titolari del trattamento dal Garante per la Protezione dei Dati personali e reperibile al seguente link:
https://servizi.gpdp.it/databreach/s/self-assessment.
Detto strumento supporterà l'Ufficio Privacy aziendale nel valutare se dall'incidente di sicurezza occorso si sia verificata una violazione dei dati personali.
Nell'ambito di tali verifiche, l'Ufficio esegue con urgenza i riscontri preliminari e, in caso di esito positivo, comunica alla Direzione Generale, ai Servizi Informativi istituiti presso il Dipartimento Sanità Digitale e Innovazione Tecnologica di ARES Sardegna nonchè alla Sc Area Tecnologia e Transizione Digitale dell'Asl Gallura l'avvenuta violazione, con trascrizione nella *scheda evento* dei dati contenuti nella scheda segnalazione di cui all'**allegato 2** recante la specifica indicazione delle seguenti informazioni, ove disponibili:
SCHEDA EVENTO
(*Riportare le seguenti informazioni*)

- la Struttura coinvolta;
- la data dell'evento e l'ora della violazione anche solo presunta (specificando se è presunta);
- la data e ora in cui si è avuto conoscenza della violazione;

- la fonte di segnalazione;
- la natura dell'evento anomalo;
- una sintetica descrizione dell'evento anomalo;
- il numero e la categoria di interessati coinvolti;
- la categoria e il volume di dati personali di cui si presume la violazione;
- la descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione;
- indicazione dell'eventuale Responsabile del trattamento coinvolto nella gestione del sistema informatico;
- misure di sicurezza, tecniche e organizzative adottate nell'ambito dei trattamenti che abbiano determinato la violazione;
- misure proposte per la mitigazione della presunta violazione;
- esito della autovalutazione eventualmente condotta mediante lo strumento messo a disposizione dal Garante per la Protezione dei Dati Personali.

Qualora la violazione sia stata riscontrata dal responsabile del trattamento, le verifiche del caso saranno poste in essere dal responsabile medesimo, che provvederà a darne tempestiva comunicazione tramite mail dedicata all'Ufficio Privacy aziendale.
Dal momento della ricezione di tale comunicazione da parte dell'Ufficio Privacy aziendale, decorrono le tempistiche (72 ore) previste dal Regolamento UE 2016/679 per la gestione degli adempimenti connessi alle violazioni accertate.

8. Valutazione e mitigazione

L'Ufficio Privacy aziendale, ricevuta la comunicazione della violazione, valuta congiuntamente al Responsabile Protezione Dati la complessità della stessa, basandosi sulle informazioni ricevute e provvede ad aggiornare la scheda evento di cui al precedente punto 7, avvalendosi della collaborazione delle Strutture a qualunque titolo interessate dalla violazione.

La violazione è definita complessa quando:

- abbia dato luogo alla violazione di dati personali *latu sensu,* ovvero abbia avuto ad oggetto l'accesso a documenti d'identità ovvero a documentazione contenente dati identificativi di uno o più soggetti interessati;

- i dati personali oggetto di violazione afferiscano alle categorie particolari di cui all'art. 9 del Regolamento UE ovvero si riferiscano a reati, condanne penali, misure di sicurezza di cui all'art. 10 dello stesso Regolamento ovvero a dati reddituali, patrimoniali e e/o di natura finanziaria;
- i sistemi informatici oggetto di violazione sono complessi per qualità/quantità di informazioni elaborate;
- comprenda le chiavi di accesso/cifratura in possesso degli interessati (i.e. password).

Nel caso in cui non ricorrano le caratteristiche di cui sopra, ossia qualora i sistemi informativi coinvolti siano limitati e/o protetti da misure adeguate (es. cifratura), o qualora non siano coinvolti interessati, se non in numero limitato e i dati personali siano parziali e non associati ad altre informazioni (es. nome e cognome senza codice fiscale o carta di credito o numeri telefonici), la violazione può essere definita non complessa.
In questa fase, l'Ufficio Privacy aziendale, in caso di dubbi sulla valutazione, sceglierà lo scenario di maggior tutela per gli interessati.
Per ciascuna violazione dei dati personali, anche avvalendosi del supporto dei Servizi Informativi istituiti presso il Dipartimento Sanità Digitale e Innovazione Tecnologica di ARES Sardegna, devono essere identificate opportune misure correttive tecniche e organizzative da adottare, al fine di mitigare i relativi effetti e ridurre la probabilità di impatto e ricorrenza. Le misure di mitigazione dovranno essere adeguate alla natura della violazione dei dati personali.
Nelle attività di valutazione dell'evento e di individuazione di misure di mitigazione e di rimedio l'Ufficio Privacy aziendale si avvale della consulenza e del supporto tecnico del Responsabile della Protezione dei Dati.
Nell'ipotesi in cui risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, ossia la violazione sia stata ritenuta non complessa, il Titolare del Trattamento non è tenuto a notificare la violazione all'Autorità Garante, pur restando fermo il dovere di censire il *data breach* all'interno del registro delle violazioni.

9. Notifica all'Autorità Garante

Qualora, alla luce delle risultanze dell'istruttoria condotta dall'Ufficio Privacy aziendale risulti probabile che il *data breach* possa rappresentare un rischio per i diritti e le libertà degli interessati, ossia la violazione sia stata ritenuta complessa, il Titolare del trattamento è tenuto a notificare l'avvenuta violazione di dati personali all'Autorità Garante entro 72 ore dal ricevimento della segnalazione da parte dell'Ufficio competente all'indirizzo ***databreach@aslgallura.it***.

Viste le risultanze istruttorie, il Responsabile della protezione dei dati esprime parere circa la necessità e l'opportunità di notificare l'avvenuta violazione all'Autorità Garante e di comunicare la stessa agli interessati, senza ritardo, stante la necessità di notificare la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il titolare del trattamento è venuto a conoscenza della violazione. A tale scopo, il RPD, con l'ausilio Ufficio Privacy aziendale, ha la facoltà di svolgere ulteriori riscontri necessari a completare le evidenze mancanti rispetto alle prime analisi condotte, avvalendosi dei Servizi Informativi istituiti presso il Dipartimento Sanità Digitale e Innovazione Tecnologica di ARES Sardegna. Il parere reso in conformità alle disposizioni di cui al presente paragrafo è annotato nella scheda evento di cui al paragrafo 7.

Il Titolare del trattamento, ricevuto il parere del RPD, invia la comunicazione all'Autorità Garante entro e non oltre le 72 ore dal ricevimento della segnalazione sulla casella di posta deputata *databreach@aslgallura.it*, tramite l'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/.

Il parere del RPD non ha carattere né obbligatorio né vincolante, sicché il Titolare è tenuto, in ogni caso, a notificare la violazione al Garante ogni qual volta lo ritenga opportuno, motivando le sue valutazioni all'interno dell'apposita scheda evento.

I tempi di notifica, nonché l'oggetto delle comunicazioni inviate al Garante devono essere formalizzati all'interno del registro delle violazioni.

Nelle ipotesi in cui il Titolare versi nel dubbio circa la complessità del *data breach* e ritenga necessari ulteriori riscontri, oltre il termine di 72 ore dal ricevimento della segnalazione sulla casella di posta deputata, è tenuto a comunicare comunque gli estremi della violazione all'Autorità Garante, indicando nella notifica stessa le informazioni in suo possesso e il termine entro il quale si ritiene termineranno le ulteriori attività istruttorie. Una volta compiute le verifiche necessarie, dovrà essere inviata una seconda comunicazione al Garante (integrazione della notifica), in cui verranno illustrati gli esiti dei successivi riscontri effettuati e le valutazioni compiute in ordine alle conseguenze e ai potenziali rischi dell'avvenuta violazione.

10. Comunicazione agli interessati

Qualora, in esito alla valutazione operata dall'Ufficio Privacy aziendale, dovesse riscontrarsi un rischio elevato per i diritti e le libertà delle persone fisiche, l'Ufficio deputato con il supporto del RPD, informato il Titolare del Trattamento, predispone la comunicazione agli interessati e la comunica senza ingiustificato ritardo, avvalendosi dei competenti Sistemi Informativi incardinati nel Dipartimento Sanità Digitale e Innovazione di ARES Sardegna.

Qualora la comunicazione risulti necessaria, saranno adottate le seguenti misure:

- l'Ufficio Privacy aziendale, previa consultazione con il RPD e in coordinamento con quest'ultimo, comunica la violazione agli interessati, entro 5 giorni dalla scoperta della violazione;
- la comunicazione avviene preferibilmente su base individuale per e-mail, salvo che sia impossibile procedere in tal modo, nel qual caso la comunicazione viene effettuata tramite il sito internet dell'ASL Gallura e/o tramite intranet aziendale;
- la comunicazione all'interessato deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali, come da **modello allegato 3**, e contenere almeno le seguenti informazioni:
    - una descrizione della natura della violazione;
    - il nome e i dati di contatto del RPD o di altro punto di contatto;
    - una descrizione delle probabili conseguenze della violazione;
    - una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Si rammenta che, ai sensi dell'art. 34, par. 3 del Regolamento, non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

1) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
2) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
3) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Nel caso in cui il Titolare del trattamento abbia deciso di non comunicare la violazione di dati personali agli interessati, deve far menzione all'interno del registro delle violazioni delle ragioni a fondamento della propria decisione. In tal caso, l'Autorità di controllo, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà degli interessati, può chiedere che il Titolare del trattamento provveda alla comunicazione ovvero può ritenere che una delle condizioni più sopra menzionate sia soddisfatta.

11. Aggiornamento del registro delle violazioni

Il Titolare del trattamento, con il supporto dell'Ufficio Privacy, una volta terminate le fasi precedenti, procede all'aggiornamento del registro delle violazioni. Segnatamente, il registro dovrà contenere le seguenti informazioni:

a) Codice Identificativo *data breach*;
b) Data in cui è avvenuta la violazione;
c) Data, orario e modalità in cui si è avuta conoscenza della violazione;
d) Natura e causa della violazione;
e) Descrizione del *data breach*;
f) Categoria di interessati coinvolti;
g) Numero di interessati coinvolti (anche approssimativo);
h) Categoria di dati personali coinvolti;
i) Numero di dati personali coinvolti (anche approssimativo);
j) Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione;
k) Misure di sicurezza tecniche e organizzative adottate al momento della violazione;
l) Responsabili del trattamento coinvolti, ove applicabile;
m) Possibili conseguenze della violazione sugli interessati;
n) Potenziali effetti negativi per gli interessati;
o) Azioni intraprese in risposta all'incidente per mitigare il danno e ridurre la probabilità di una recidiva simile;
p) Stima della gravità della violazione;
q) Indicazione dell'avvenuta notifica all'Autorità Garante (nei casi in cui non si sia proceduto con tale notifica, è necessario specificarne le ragioni);
r) Comunicazione della violazione agli interessati (ove necessario);

s) Numero di interessati a cui è stata comunicata la violazione;
t) Canale utilizzato per la comunicazione agli interessati;
u) Eventuale notifica ad altre autorità di controllo, organismi di vigilanza o di controllo o all'autorità giudiziaria o di polizia.

12. Definizione del piano di rimedio

Una volta concluso il processo di notifica e comunicazione della violazione di dati personali agli interessati, il Titolare del trattamento, avvalendosi dell'Ufficio Privacy aziendale, del RPD e con il supporto dei competenti Sistemi Informativi incardinati nel Dipartimento Sanità Digitale e Innovazione di ARES Sardegna, svolge le seguenti attività:

- analizza le cause che hanno determinato la violazione di dati personali;
- valuta le opportunità di miglioramento dei presidi e dei processi di monitoraggio delle violazioni dei dati personali, al fine di mettere in atto misure tecniche e organizzative adeguate a garantire il rispetto del Regolamento;
- definisce un piano di rimedio al fine di garantire un livello di sicurezza adeguato ai rischi in ordine alla protezione dei dati personali trattati.

Per ciascuna violazione di dati personali, il Titolare del trattamento è tenuto a verificare se l'incidente è il risultato di un errore umano o di un problema di natura tecnica o organizzativa e valutare misure correttive volte a prevenire il ripetersi dell'evento. È, altresì, necessario che il Titolare del trattamento preveda attività di verifica periodiche volte a garantire l'efficacia delle procedure e degli strumenti di risposta agli incidenti relativi alle violazioni di dati personali.

Allegati

- All. 1: Registro delle violazioni;
- All. 2: Scheda segnalazione dell'evento;
- All. 3: modello comunicazione all'interessato;