Procedura per la gestione di Data Breach ai sensi del GDPR (Regolamento Europeo 679/2016) nell'ASL AT.

Sommario

PREMESSA

Il Regolamento Europeo 679/2016 (di seguito anche "Regolamento" o "GPDR") introduce una norma specifica sulla notifica della violazione dei dati personali (c.d. Data Breach) al Garante Nazionale e, in certi casi, alla persona che ha subito tale violazione.

Questo perché una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Il presente documento si prefigge lo scopo di indicare alla ASL AT le opportune modalità di gestione del Data Breach, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento e definendo i passaggi e controlli demandati all'Ufficio Audit Privacy richiesti per la notifica della violazione stessa.

In questo documento si sintetizzano le regole per garantire il rispetto dei principi esposti e la realizzabilità tecnica e la sostenibilità organizzativa, nella gestione del data breach, sotto i diversi aspetti relativi a:

- *modalità e profili di segnalazione al Titolare per il tramite sia ai designati e sia ai Responsabili del trattamento dati;*
- *modalità e profili di segnalazione all'Autorità Garante;*
- *valutazione dell'evento accaduto;*
- *eventuale comunicazione agli interessati.*

È necessario che ASL AT dia notizia a tutti i dipendenti e/o collaboratori in merito alla presente procedura mediante idonea delibera e/o circolare.

Nell'ASL AT è individuato il Responsabile Dati ovvero colui che avvia il procedimento e può avvalersi della consulenza del DPO e ove opportuno della Commissione Privacy.

NORMATIVA E DOCUMENTI DI RIFERIMENTO

- Regolamento UE 679/2016, considerando n. 85, 86, 87, 88 artt. 33, 34
- Decreto Legislativo n. 101 del 10/08/2018
- Guidelines on Personal Data Breach notification under Regulation 2016/679 – article 29 data protection working party (Adopted on 3 October 2017 – as last Revised and Adopted on 6 February 2018), incluso il WP 250.

GLOSSARIO

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, punto 7). In questo contesto è titolare del trattamento il direttore generale del ASL AT.

GDPR o Regolamento: Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679.

Pseudonimizzazione: il Trattamento dei Dati Personali in modo tale che i Dati Personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile;

Responsabile del Trattamento Dati: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;

Designato interno: Direttore/responsabile di struttura o altra figura, individuata secondo quanto previsto nel Regolamento aziendale privacy, ai sensi dell'art. 2 – quaterdecies, comma 1, del Codice Privacy dal Titolare del trattamento per la capacità, l'esperienza e la formazione in funzione dell'incarico ricoperto, con l'attribuzione dei compiti e delle funzioni specificatamente previste nell'atto di nomina;

Data Protection Officer (c.d. DPO): la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).

Commissione Privacy: gruppo multidisciplinare di professionisti che supportano il titolare e i responsabili privacy per specificità tecniche quali ICT, SIC, area giuridica, area del personale, ecc..

Violazione dei dati personali (c.d. Data breach):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**;**

Gruppo Audit Privacy: gruppo multidisciplinare di professionisti che supportano il titolare alla gestione del Data Breach, massimo 4 persone, di cui una risorsa con competenze informatiche, una di gestione del rischio, una sanitario, oltre il supporto specifico del DPO.

MODALITÀ E PROFILI DI NOTIFICA ALL'AUTORITÀ GARANTE PRIVACY

FASE 1: RACCOLTA DELLE INFORMAZIONI

A. CANALI INTERNI

Le segnalazioni interne di eventi anomali e/o presunte violazioni possono pervenire dal personale interno/esterno dell'Azienda; in questo caso il personale deve segnalare l'accaduto al designato, il quale tramite la compilazione della Scheda Evento (Allegato B) comunica all'Ufficio Audit Privacy la presunta violazione. Tale comunicazione deve esser fatta entro le 12 ore dalla conoscenza della presunta violazione.

B. CANALI ESTERNI

Le segnalazioni possono pervenire anche da fonti esterne, ogni interessato, anche solo in caso di sospetto, può tramite PEC (protocollo@pec.asl.at.it) o su segnalazione all'U.R.P., comunicare il dubbio che i propri dati personali siano stati utilizzati abusivamente o fraudolentemente da un terzo e che ci sia stata una violazione della privacy.

La segnalazione viene inoltrata al Gruppo Audit Privacy che compila la scheda evento e la comunica al DPO per eventuale consulenza.

FASE 2 - ANALISI DELLE SEGNALAZIONI

A. ANALISI PRELIMINARE ED ELABORAZIONE DELLA SCHEDA EVENTO

Il designato, avuta comunicazione della presunta violazione, avvia un'analisi preliminare finalizzata alla raccolta dei dati concernenti l'anomalia e alla compilazione della Scheda Evento contenente tutte le informazioni raccolte.

La Scheda Evento viene inviata al Gruppo Audit Privacy (entro e non oltre le 12 ore) quindi destinata all'analisi di primo livello descritta di seguito.

B. ANALISI DI PRIMO LIVELLO - VERIFICA DELLA SEGNALAZIONE

Obiettivo dell'analisi di primo livello è quella di verificare che la segnalazione non integri un cd. "falso positivo".

Il Gruppo Audit Privacy cura l'istruttoria per l'analisi di primo livello al fine di verificare se l'evento costituisca un "falso positivo"o che si tratti di un data breach, anche attraverso la procedura di autovalutazione disponibile sul sito del Garante per la protezione dei dati personali.

L'istruttoria dovrà essere condivisa con il D.P.O. e comunicata al Titolare per le successive decisioni.

Acquisita la decisione in ordine alla sussistenza di un "falso positivo" si chiude l'incidente, il Gruppo Audit Privacy si attiva per effettuare un raffinamento delle regole di rilevazione dei falsi positivi e inserisce l'evento nel Registro dei Data Breach, nella apposita sezione dedicata agli "eventi falsi positivi". Al termine dell'anno solare sarà redatto un report sui "falsi positivi".

Nel caso in cui l'evento risulti “positivo”, il Gruppo Audit Privacy recupera le informazioni di dettaglio necessarie alle analisi di secondo livello e le riporta nella Scheda Violazione Dati (Allegato C).

C. ANALISI DI SECONDO LIVELLO - SCHEDA VIOLAZIONE DATI

Svolta l’analisi di primo livello con esito che non si tratta di un “falso positivo”, il Gruppo Audit Privacy analizza congiuntamente tutte le informazioni raccolte e redige la Scheda Violazione Dati in collaborazione con il DPO, i designati e ove occorre con i membri della Commissione Privacy o con tecnici aziendali.

Inoltre il Gruppo Audit Privacy deve proporre, in accordo con il DPO, le misure da adottare che consentano di minimizzare le conseguenze negative della violazione.

FASE 3: NOTIFICA, SEGNALAZIONI E COMUNICAZIONE

A. NOTIFICA ALLA AUTORITÀ DI CONTROLLO

Redatta la Scheda Violazione Dati, il Gruppo Audit Privacy deve valutare le azioni da intraprendere ed avviare la notificazione verso l'Autorità di Controllo e, ove necessario, la comunicazione agli interessati, verificando e validando la documentazione pervenuta dalle precedenti fasi di lavoro.

Il Titolare notifica la violazione all'Autorità di Controllo competente senza ingiustificato ritardo entro 72 ore dal momento in cui è venuto a conoscenza, a meno che sia improbabile che la Violazione dei Dati Personali presenti un rischio per i diritti e le libertà delle persone fisiche e dunque sia stato dallo stesso classificato “NULLO” e quindi un “falso positivo”.

Qualora la notifica all'Autorità di Controllo non sia effettuata entro 72 va corredata dei motivi del ritardo.

La notifica all’Autorità di Controllo deve descrivere, ove possibile:

- La natura della violazione dei dati personali compresi
    1. Le categorie e il numero approssimativo di interessati in questione
    2. Le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
    3. Comunicare il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
- Descrivere le probabili conseguenze della violazione dei dati personali;
- Descrivere le misure adottate o di cui si propone l'adozione da parte della ASL AT per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

L'ASL AT notifica la violazione dei dati personali in modalità telematica, secondo la procedura adottata dal Garante per la protezione dei dati personali con il provvedimento n. 209 del 27 maggio 2021. L’adempimento è assolto dal legale rappresentante quale <Utente non autenticato>.

B. SEGNALAZIONI AD ALTRE AUTORITA'

Il Titolare, qualora necessario, effettua la segnalazione dell'accaduto anche ad altre Autorità. In particolare in caso di incidenti informatici, ai sensi della circolare Agid n. 2/2017 del 18 aprile 2017 informa CERT-PA e in caso di violazioni di dati in conseguenza di comportamenti illeciti o fraudolenti gli Organi di Polizia.

C. COMUNICAZIONE DELLA VIOLAZIONE ALL'INTERESSATO

Il Titolare sentito il Gruppo Audit Privacy, deve informare gli interessati dell'evento anomalo, in tutti i casi in cui, a norma degli artt. 33-34 GDPR, il Gruppo Audit Privacy valuti che la violazione risulta presentare rischi classificati come "ALTI" nella Scheda Violazione Dati per i diritti e le libertà delle persone fisiche.

La comunicazione deve essere rivolta alla persona fisica cui riferiscono i dati personali e particolari oggetto di trattamento ("Interessato") senza ingiustificato ritardo dall'avvenuta conoscenza e valutazione della violazione, attraverso il canale di comunicazione ritenuto più idoneo; deve essere effettuata ad opera del Gruppo Audit Privacy e deve essere intellegibile, coincisa, trasparente e facilmente accessibile; deve essere utilizzato un linguaggio semplice e chiaro adottando, se possibile, la stessa lingua parlata dall'Interessato.

La comunicazione di Data Breach all'Interessato deve contenere le seguenti informazioni:

1. Data e ora della violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa;
2. La natura della violazione dei dati personali;
3. Il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
4. Le probabili conseguenze della violazione dei dati personali;
5. La descrizione delle misure adottate o di cui si propone l'adozione da parte della ASL AT per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

- Sono state messe 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; salvo i casi in cui la violazione della sicurezza ha comportato la distruzione o la perdita dei Dati Personali degli Interessati;
- Sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà delle persone fisiche – in tal caso è necessario documentare le misure nella scheda di violazione;

- 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.

Il Gruppo Audit Privacy riporta in calce la comunicazione all'Interessato della Violazione dei Dati Personali.

FASE 4: REGISTRAZIONE NEL REGISTRO DEI DATA BREACH

Nel Registro dei Data Breach, il Gruppo Audit Privacy documenta ogni singolo evento, sia esso "falso" o "positivo";

Tale documentazione consente all'Autorità di Controllo di verificare il rispetto delle norme in materia di notificazione delle Violazioni di Dati Personali. Il Registro dei Data Breach è tenuto a cura del Gruppo Audit Privacy ai sensi dell'art. 33, comma 5 del GDPR.

FASE 5: ANALISI POST VIOLAZIONE

L'ultima fase del processo di gestione delle Violazioni di Dati Personali prevede la raccolta finale delle evidenze, l'analisi delle informazioni giunte sul contesto di violazione osservato, e la valutazione delle stesse al fine di effettuare un'analisi post-incidente, per verificare l'efficacia e l'efficienza delle azioni intraprese durante la gestione dell'evento ed identificare possibili aree di miglioramento. Tale valutazione deve esser fatta in collaborazione con il DPO che coinvolgerà la struttura coinvolta, con eventuale supporto da parte di altre aree funzionali e tecniche.

DATA BREACH PRESSO LA SOCIETÀ O UN TERZO IN QUALITÀ DI RESPONSABILE

PREMESSA

Ogniqualvolta l'ASL AT si trovi ad affidare il trattamento di dati ad un soggetto terzo/responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto o atto giuridico che lo vincoli al rispetto delle istruzioni impartitegli dal titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di data breach sia inclusa nel suddetto contratto. Ciò al fine di obbligare il responsabile ad informare il titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di data breach.

Ad ogni responsabile del trattamento deve essere comunicato il contatto del Gruppo Audit Privacy al quale effettuare la predetta segnalazione via email o preferibilmente via PEC; dovrà essere altresì reso noto il contatto del DPO dell'ASL AT.

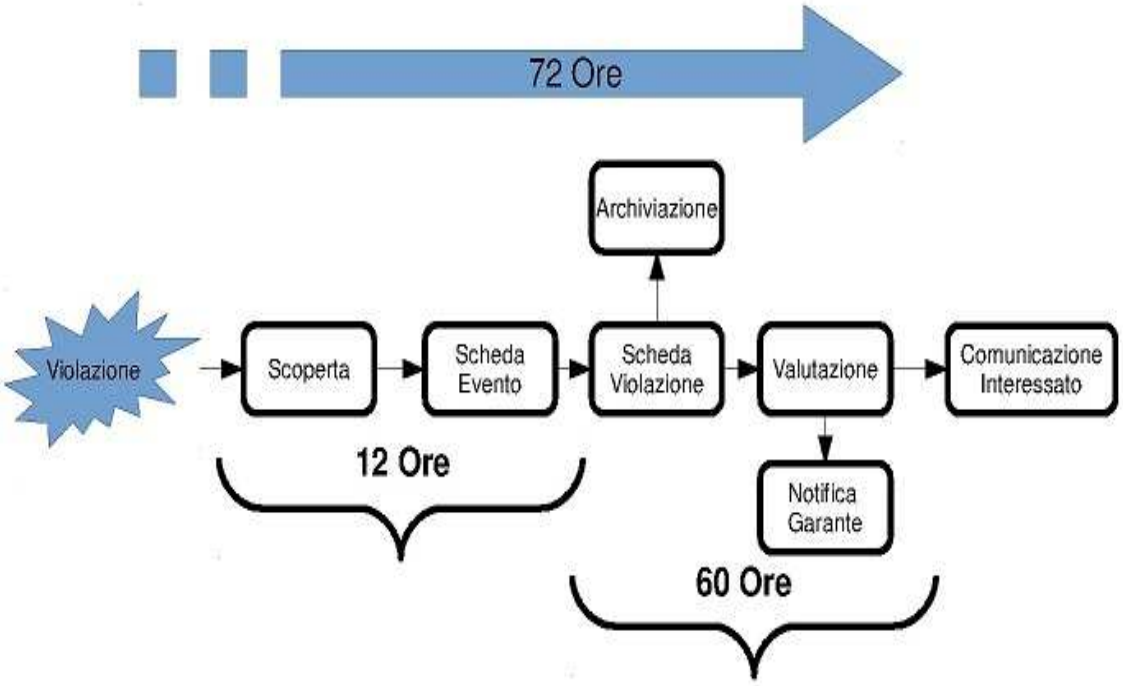
A. OBBLIGHI DI COMUNICAZIONE DELLA SOCIETÀ ESTERNA QUANDO OPERA IN QUALITÀ DI RESPONSABILE

Quando la Società esterna agisce in qualità di Responsabile, in caso di Violazione dei Dati Personali, deve informare il Titolare (solitamente il cliente per il quale offre servizi) per il tramite del Gruppo Audit Privacy, senza ingiustificato ritardo secondo i tempi e i modi concordati nel contratto per il trattamento dei dati personali trasmesso da quest'ultimo e comunque entro le 12 ore.

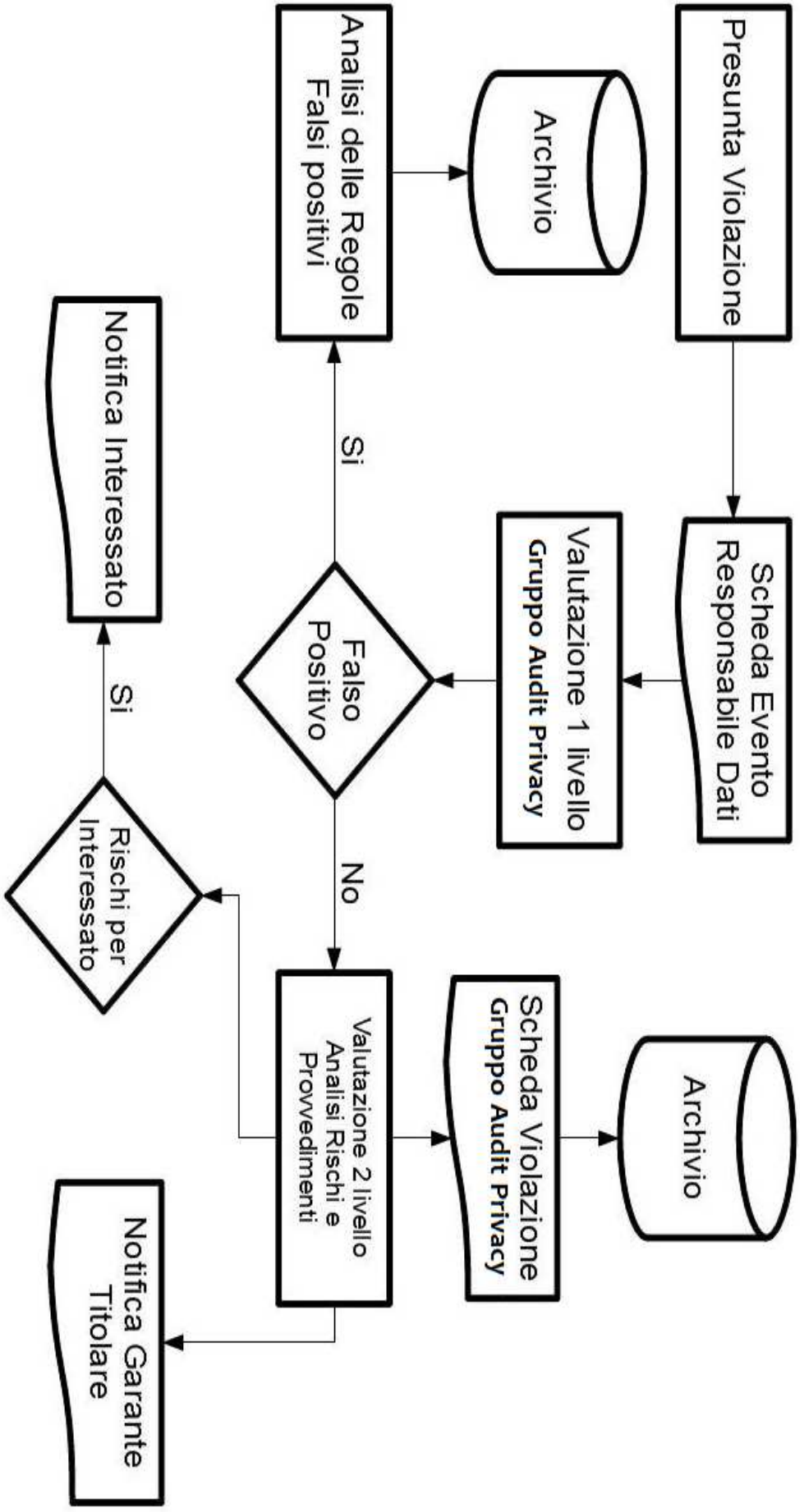
B. OBBLIGHI DI COMUNICAZIONE DI UN RESPONSABILE NEI CONFRONTI DELLA SOCIETÀ ESTERNA

Quando un terzo agisce in qualità di Responsabile del trattamento dati (cfr. Linee guida sul Responsabile del Trattamento), in caso di Violazione dei Dati Personali, deve informare ASL AT (che agisce in qualità di Titolare), senza ingiustificato ritardo e **non al più tardi di 12 ore dal momento in cui ha conoscenza della violazione**, inviando una comunicazione ai seguenti indirizzi, ove possibile via PEC (protocollo@pec.asl.at.it) e successivamente collaborare con ASL AT esterna per consentirgli di adempiere agli obblighi previsti dalla normativa agli artt. 33 e 34 GDPR.

La procedura che segue è la stessa del Canale Interno come sopraindicato, salvo accordi contrattuali diversamente concordati dal ASL AT.


72 Ore
Archiviazione
Violazione
Scoperta
Scheda Evento
Scheda Violazione
Valutazione
Comunicazione Interessato
12 Ore
Notifica Garante
60 Ore

Flow Chart


Presunta Violazione
Scheda Evento Responsabile Dati
Valutazione 1 livello Gruppo Audit Privacy
Falso Positivo
Si
Analisi delle Regole Falsi positivi
Archivio
Notifica Interessato
Si
Rischi per Interessato
No
Valutazione 2 livello Analisi Rischi e Provvedimenti
Scheda Violazione Gruppo Audit Privacy
Archivio
Notifica Garante Titolare

Allegato A: Schema di valutazione scenari – data breach

Di seguito sono illustrati alcuni esempi, non esaustivi, di possibili violazioni di dati personali, allo scopo di supportare i soggetti coinvolti nella procedura, nella valutazione in merito alla necessità di effettuare o meno la notifica di data breach all'Autorità Garante.

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	• Rottura dell'ecografo prima di inviare al sistema centrale l'immagine. • Guasto non riparabile dell'hard disk contenente uno o più referti che, in violazione al regolamento, erano salvati localmente • Incendio di archivio cartaceo delle cartelle cliniche. • Distruzione di campioni biologici	• Rottura di una chiavetta USB che non contiene dati personali originali (in unica copia) • Rottura di un PC che non contiene dati personali originali (in unica copia) • Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo
Perdita	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili • Dati relativi a più assistiti, relativi a interi episodi o relativi a tipologie di dato la cui indisponibilità lede i diritti fondamentali dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamentali dell'interessato Rientrano tra i casi di	• Smarrimento di chiavetta USB contenente dati originali • Smarrimento di fascicolo cartaceo personale dipendente	• Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
		segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione		
Modifica	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	Caratteristiche: • Modifiche sistematiche su più casi Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Guasto tecnico che altera parte dei contenuti di un sistema clinico, compromettendo anche i backup • Azione involontaria, o fraudolente, di un utente che porta alla alterazione di dati sanitari in modo non tracciato e irreversibile	• Guasto tecnico che altera parte dei contenuti di un sistema clinico, rilevato e sanato tramite operazioni di recovery • Azione involontaria di un utente che porta alla alterazione di dati tracciata e reversibile • Modifica di un documento non ancora validato dal proprio autore.
Divulgazione non Autorizzata	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Malfunzionamento del sistema di oscuramento del sistema dipartimentale che invia a SOLE • Consegna di un CD con dati dei pazienti ad altra struttura senza autorizzazione	• Il medico sul proprio sistema dipartimentale seleziona il paziente Mario Rossi ma visita il paziente Luca Bianchi. Inserisce anamnesi e gli altri valori di refertazione ed invia a SOLE. • Infezione virale di un PC con un virus che dalla scheda tecnica non trasmette dati su internet • Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
Accesso non Autorizzato	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi • Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema clinico	• Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi • Accesso non autorizzata di un documento non ancora validato dal proprio autore.
Indisponibilità temporanea del dato	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato.	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale	• Infezione da ransomware che comporta la temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal backup • cancellazione accidentale dei dati da parte di una persona non autorizzata • perdita della chiave di decrittografia di dati crittografati in modo sicuro • irraggiungibilità di un sito di stoccaggio delle cartelle cliniche poste in montagna per isolamento neve	• Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso

Un data breach, quindi, non è solo un attacco informatico, ma può consistere anche in un accesso abusivo, un incidente (es. un incendio o una calamità naturale), nella semplice perdita di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno), nella sottrazione di documenti con dati personali (es. furto di un notebook di un dipendente). I casi di data breach per

le casistiche già descritte si estendono ai documenti cartacei o su supporti analogici. La comunicazione involontaria di documenti, o in generale di dati, che non abbiano vero senso compiuto/riconducibilità verso l'interessato non è considerato data breach, ma è considerato un normale errore procedurale.

Questo poiché:

- Chi riceve non può sapere a quale paziente fisico è riferito il testo;
- Il paziente fisico non è danneggiato poiché nessuno riferimento alla sua persona è stato diffuso.

Allegato B: Scheda Evento

Data e ora rilevazione	
Data e ora segnalazione	
Soggetto segnalante	*(Nome e cognome, qualifica)*
Struttura di appartenenza	
Recapiti	*(mail, numero cellulare)*
Processi/servizi segnalati	

Modalità di esposizione al rischio:

Indicazioni circa la violazione percepita:

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- ☐ Altro ……..

Indicazioni circa il dispositivo oggetto della violazione

- ☐ PC
- ☐ Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di back up
- ☐ Documento cartaceo
- ☐ Altro :……..

Ubicazione del dispositivo: ……..

Indicazioni circa il tipo di dato oggetto di violazione se già individuabile:

- ☐ Dati personali
- ☐ Indirizzo di posta elettronica
- ☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
- ☐ Dati che rivelino l'origine razziale o etnica
- ☐ Dati che rivelino opinioni politiche, convinzioni religiose
- ☐ Dati che rivelino l'appartenenza sindacale
- ☐ Dati genetici
- ☐ Dati biometrici
- ☐ Dati relativi alla salute

- ☐ Dati relativi alla vita sessuale o all'orientamento sessuale
- ☐ Dati relativi a minori
- ☐ Dati sanitari relativi a persone sieropositive, a donne sottoposte a IVG, a vittime di atti di violenza sessuale o pedofilia, a persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, a donne che partoriscono in anonimato
- ☐ Copie per immagine su supporto informatico di documenti analogici
- ☐ Altro ……

Numero di interessati coinvolti se già quantificabile: .....

L'incidente è stato causato dalle seguenti cause:

- ☐ Accesso a sistemi o informazioni da parte di utenti non autorizzati
- ☐ Furto o diffusione di informazioni
- ☐ Furto o smarrimento di dispositivi
- ☐ Uso inappropriato
- ☐ Virus o malware
- ☐ Attacchi hacking
- ☐ Negazione di servizio
- ☐ Errori umani
- ☐ Procedure inappropriate
- ☐ Altro ……

L'incidente è occorso presso un Responsabile Esterno di trattamento dei dati personali?

· SI · NO

Se Responsabile Esterno specificare i trattamenti oggetto di nomina:

Breve descrizione dell'evento

Data	Firma del responsabile del trattamento dati

Allegato C: Scheda Violazione

Data e ora rilevazione

Data e ora segnalazione

Responsabile Trattamento dati *(Nome e cognome, qualifica)*

Struttura di appartenenza

Scheda Evento *(Numero identificativo della Scheda Evento)*

Livello di Rischio

Falso Positivo		Positivo	
▪ NULLO	▪ BASSO	▪ MEDIO	▪ ALTO

Classificazione dell'Evento

- ☐ Distruzione di dati illecita;
- ☐ Perdita di dati illecita;
- ☐ Modifica di dati illecita;
- ☐ Distruzione di dati accidentale;
- ☐ Perdita di dati accidentale;
- ☐ Modifica di dati accidentale;
- ☐ Divulgazione non autorizzata;
- ☐ Accesso ai dati personali illecito;
- ☐ Accesso ai dati particolari illecito;
- ☐ Altro ……..

Tipologia del rischio

- ☐ Discriminazioni;
- ☐ Furto o usurpazione d'identità;
- ☐ Perdite finanziarie;
- ☐ Pregiudizio alla reputazione;
- ☐ Perdita di riservatezza dei dati particolari da segreto professionale;
- ☐ Decifratura non autorizzata della pseudominizzazione;
- ☐ Privazione o limitazione dei diritti o libertà;
- ☐ Impedito controllo sui dati personali e particolari dell'interessato;
- ☐ Danni fisici, materiali o immateriali alle persone fisiche;
- ☐ Altro ……..

Tipologia dei dati

- ☐ Che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati

relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;

- ☐ Che si tratti di dati relativi a valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- ☐ Che si tratti di dati di persone fisiche vulnerabili, in particolare minori;
- ☐ Che il trattamento riguardi una notevole quantità di dati personali;
- ☐ Che il trattamento riguardi un vasto numero di interessati;
- ☐ Altro …….

Sistemi ITC interessati

Trattamenti dati Interessati
(indicare il riferimento al Registro Trattamenti)

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ Persone certe n. _____
- ☐ Circa persone n. _____
- ☐ Un numero (ancora) sconosciuto di persone

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ Il _____
- ☐ Tra il _____ e il _____
- ☐ In un tempo non ancora determinato è possibile che sia ancora in corso.

Notifica al Garante

- SI in data _____ Protocollo: _____
- NO perché:

La violazione è stata comunicata anche agli interessati?

- SI in data _____ Protocollo: _____
- NO perché:

Misure tecniche e organizzative applicate ai dati oggetto di violazione

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

Data