Asl3
Sistema Sanitario Regione Liguria

Allegato "3"

POLICY AZIENDALE IN CASO DI VIOLAZIONE PRIVACY (DATA BREACH)

Rev. 2020

Asl3
Sistema Sanitario Regione Liguria

Premesse

Con il termine *data breach*, ai sensi degli artt.33 e 34 del RGPD , si intende la violazione dei dati personali dell'interessato, che può consistere, a titolo esemplificativo e non esaustivo (Considerando 85 del RGPD) in:
-perdita del controllo dei dati personali che lo riguardano o limitazione dei suoi 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
- qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Trattasi di una 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.
Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Alcuni possibili esempi:

- 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, ecc.;
- 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.

In linea con la definizione di violazione di dato personale, ex art.4 parag.12 del RGPD, si possono distinguere tre tipi di violazione, che possono anche combinarsi tra loro:
-violazione della riservatezza, quando si verifica una divulgazione o n accesso a dati personali non autorizzato o accidentale
-violazione di integrità, quando si verifica un'alterazione di dati personali non autorizzata o accidentale
-violazione di disponibilità, quando si verifica perdita, inaccessibilità o distruzione , accidentale o non autorizzata, di dati personali.

Obblighi del Titolare

Il Titolare ha l'obbligo di notificare all'Autorità di controllo (Garante Privacy) le violazioni di dati personali di cui venga a conoscenza, **entro 72 ore** e, comunque, «senza ingiustificato ritardo», soltanto nel caso in cui ritenga probabile che per tale violazione vi siano rischi per i diritti e le libertà degli interessati.
Se i predetti rischi sono valutati dal titolare come elevati, ne dovranno essere informati anche gli interessati (art.34 RGPD), a meno che il Titolare:
- Abbia messo in atto misure adeguate di protezione ai dati oggetto delle violazioni, in particolare quelle che rendono incomprensibili i dati (cifratura e/o anonimizzazione)
- Abbia messo successivamente in atto misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e libertà degli interessati.
- La comunicazione potrebbe richiedere sforzi sproporzionati. In questo caso si procede a comunicazione pubblica od a una misura simile.

Contenuti della notifica

I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati negli artt. 33 e 34 del Regolamento Europeo 679/2016.
La notifica dovrà contenere , in particolare , le informazioni previste all'art. 33, par. 3 del Regolamento (UE) 2016/679 e indicate nell'allegato al Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali .

La notifica deve essere inviata al Garante tramite posta elettronica certificata all'indirizzo **protocollo@pec.gpdp.it** (solo PEC) oppure tramite posta elettronica ordinaria all'indirizzo **protocollo@gpdp.it** e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.
L'oggetto del messaggio deve contenere obbligatoriamente la dicitura **"NOTIFICA VIOLAZIONE DATI PERSONALI"** e opzionalmente la denominazione del Titolare del trattamento ASL 3.

Il Garante, oltre a chiare indicazioni operative rinvenibili sul sito dello stesso (ww.garanteprivacy.it) ha anche fornito uno specifico format, scaricabile dal sito dello stesso, all'indirizzo:

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9128501

In particolare per la notifica il Titolare deve indicare:
-la natura della violazione compresi, ove possibile, le categorie di dati e di interessati coinvolti
-comunicare i dati di contatto del responsabile della protezione dei dati (R.P.D.) o altro punto di contatto per avere ulteriori informazioni
-descrivere le probabili conseguenze della violazione dei dati personali
-descrivere le misure adottate o che si intendono adottare per porre rimedio alla violazione ed attenuarne se possibile gli effetti negativi.
Il Titolare del trattamento, anche laddove ritenga che non ci siano rischi per i diritti e le libertà degli interessati, documenta comunque qualsiasi violazione dei dati personali, che deve contenere gli stessi elementi previsti per la notifica.

Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere **accompagnate dai motivi del ritardo.**

Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il Titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

Il Titolare del trattamento ASL 3, a prescindere dalla notifica al Garante, **documenta** tutte le violazioni dei dati personali, con un apposito **registro ("Registro delle violazioni"),** tenuto presso il RPD. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

Obblighi dei Dipendenti e/o assimilati di ASL 3 e relativa procedura per la gestione

In caso di violazione di dati personali di cui si sia venuti a conoscenza, ciascun Dipendente e/o assimilato di ASL 3 è tenuto a segnalare immediatamente e, comunque, non oltre le 24 ore, al proprio Dirigente responsabile di struttura-area, al Referente e per conoscenza al R.P.D. (all'email dedicata rpd@asl3.liguria.it) ed alla S.C. Affari Generali (e mail: segreteria.contratticonvenzioni@asl3.liguria.it) qualsiasi violazione privacy in cui ritenga probabile che per tale violazione vi siano rischi per i diritti e le libertà degli interessati.
La comunicazione deve contenere possibilmente le seguenti informazioni:
-la natura della violazione (es. lettura, copia, alterazione, cancellazione, furto, etc.) compresi, ove possibile, le categorie di dati (es. dati anagrafici, indirizzo di posta elettronica, dati di accesso o identificazione, categorie particolari di dati personali, dati di contatto, dati personali, etc.) e di interessati coinvolti (es. minori, soggetti a particolari tutele, utenti, privati, etc.), indicazioni circa l'eventuale dispositivo oggetto di violazione e la sua ubicazione (es. computer, rete, dispositivo mobile, file o parte di esso, strumento di backup, etc.)
-descrizione delle probabili conseguenze della violazione dei dati personali
-descrizione delle eventuali misure adottate o che si ritiene possano essere adottate per porre rimedio alla violazione ed attenuarne se possibile gli effetti negativi.

Particolare attenzione dovrà essere posta a servizi in *cloud,* con riguardo anche all'ubicazione del server ed alle modalità di gestione del registro dei log e degli eventi, per il rischio di accessi non autorizzati di terzi.

L'analisi della violazione da parte del Dirigente responsabile di struttura-area interessata (delegato/subdelegato del Titolare autorizzato con compiti specifici) e del Referente di riferimento viene effettuata di concerto con l'amministratore di sistema/SIA, in caso di trattamento effettuato con strumenti informatici e determina una vera e propria DPIA dell'incidente occorso, nella prospettiva della tutela dei diritti degli interessati.

Se la violazione è registrata dall'amministratore di sistema , lo stesso deve procedere come gli altri autorizzati alla segnalazione immediata al proprio Dirigente responsabile di struttura, al Referente e per conoscenza al R.P.D. ed alla S.C. Affari Generali ed all'analisi dell'incidente , come sopra illustrato.

Analoghi obblighi di segnalazione e di analisi sono previsti all'interno delle designazioni dei responsabili del trattamento ex art.28 RGPD e degli accordi di contitolarità ex art.26 RGPD.

Le risultanze dell'analisi devono essere messe a disposizione del Titolare, tramite il RPD.

Sulla base dei risultati dell'analisi:

- Se la violazione non risulta presentare alcun rischio per gli interessati il Titolare, supportato dal RPD, non effettua alcuna notifica né comunicazione. La violazione viene comunque annotata nell'apposito registro delle violazioni, motivando la scelta fatta.
- Se la violazione presenta rischi per gli interessati, nell'ambito dell'analisi si procede conformemente allo schema delle linee guida WP29 infra citato, così da stimare la gravità del rischio, per fornire al Titolare gli elementi per la notifica , supportato dal RPD, ed eventuali comunicazioni. Il *Data Breach* deve confluire nel **"Registro delle violazioni**".

Che tipo di violazioni di dati personali vanno notificate?

Vanno notificate unicamente le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali.

Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

La qualificazione della violazione quale *data breach* è, quindi, demandata al Titolare e deve tener conto tanto della qualità del dato quanto dei sistemi e misure di sicurezza posti a presidio dello stesso, per cui anche ad es. in caso di dati particolarissimi, l'adozione della misura dell'anonimizzazione potrebbe escludere la notifica della violazione.
In punto le Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018 forniscono una casistica adeguata (https://ronchilegal.eu/wp-content/uploads/2018/02/WP29-Linee-guida-su-notifica-Data-Breach-Ed.-6.2.2018.pdf).

Le azioni del Garante

Il Garante può prescrivere misure correttive (v. art. 58, paragrafo 2, del Regolamento UE 2016/679) nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione.

Sono previste sanzioni pecuniarie che possono arrivare **fino a 10 milioni di Euro** o, nel caso di imprese, **fino al 2% del fatturato totale annuo mondiale**.

Regimi particolari di Data Breach

Il Provvedimento n.331 del 4.6.2015 in materia di Dossier Sanitario Elettronico (doc.web.4084632 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4084632) ed il Provvedimento n.392 del 2.7.2015 in materia di Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche (doc.web.n.4129029 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4129029), prevedono che la notifica vada effettuata nel termine più stringente di 48 ore dalla conoscenza del fatto.

Ed il Provvedimento n.513 del 12.11.2014 in materia di biometria addirittura entro 24 ore dalla conoscenza del fatto (doc.web.3556992 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992).

In detti casi particolari sono anche indicati un indirizzo ed un modello specifico di notifica.

SCHEMA DI VALUTAZIONE DEGLI SCENARI DI DATA BREACH sulla base delle Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018 (https://ronchilegal.eu/wp-content/uploads/2018/02/WP29-Linee-guida-su-notifica-Data-Breach-Ed.-6.2.2018.pdf).
Per *data breach* si intende qualsiasi accesso abusivo (non necessariamente informatico), incidente (es. incendio, alluvione, calamità naturale, etc.), perdita di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno, etc.), sottrazione di documenti contenenti dati personali (es. furto di un notebook, etc.) e può riguardare sia documenti cartacei che su supporti analogici.
Non si considera invece tale la comunicazione involontaria di dati che non siano riconducibili all'interessato.
A titolo esemplificativo e non esaustivo, rientrano in detta categoria:

TIPO DI DATA BREACH	DEFINIZIONE	ESTENSIONE MINIMA/SOGLIA DI SEGNALAZIONE	ESEMPI	ESEMPI DI CASI ESCLUSI
Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del Titolare né di altri. Non sarebbe pertanto possibile fornire il dato all'interessato a sua richiesta	Caratteristiche: dati non recuperabili o provenienti da procedure non ripetibili. Deve trattarsi di dati appartenenti a documenti definitivi e già dotati di un livello minimo di validazione.	Guasto non riparabile dell'hard disk contente dati particolari, salvati localmente Incendio di archivio cartaceo di cartelle cliniche/fascicoli personali dei dipendenti Distruzione di campioni biologici	Rottura di una chiavetta USB/di un PC non contenente dati personali in unica copia Distruzione di un documento in corso di stesura nell'apposito applicativo, ad es. per guasto del sistema
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 no). Non sarebbe pertanto possibile fornire il dato all'interessato a sua richiesta 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 utenti, a interi episodi o tipologie di dato la cui indisponibilità lede i diritti fondamentali dell'interessato o la cui divulgazione conseguente alla perdita può ledere i diritti fondamentali dell'interessato. Deve trattarsi di dati appartenenti a documenti definitivi e già dotati di un livello minimo di validazione.	Smarrimento chiavetta USB contenente dati originali. Smarrimento di fascicolo cartaceo personale dipendente.	Smarrimento di un documento , ad es. a causa di un guasto di sistema , dopo la stampa.
Modifica	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato , senza possibilità di ripristinare lo stato originale. Non sarebbe pertanto possibile fornire il dato all'interessato a sua richiesta con la certezza che non sia stato modificato	Caratteristiche: modifiche sistematiche su più dati. Deve trattarsi di dati appartenenti a documenti definitivi e già dotati di un livello minimo di validazione.	Guasto tecnico che altera parte dei contenuti di un sistema clinico, compromettendo anche i backup. Azione involontaria o fraudolenta di un utente che porta all'alterazione di dati sanitari in modo non tracciato ed irreversibile.	Guasto tecnico che altera parte dei contenuti di un sistema clinico, rilevato e sanato tramite operazioni di *recovery*. Azione involontaria o fraudolenta di un utente che porta all'alterazione di dati in modo tracciato e reversibile. Modifica di documento non ancora validato dal suo autore.
Divulgazione non autorizzata	Un insieme di dati personali (e riconducibili all'interessato direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terzi senza il consenso dell'interessato , se dovuto, o in violazione di legge/regolamento	Deve trattarsi di dati appartenenti a documenti definitivi e già dotati di un livello minimo di validazione.	Consegna di un supporto mobile con dati di utenti ad altra struttura senza consenso, se dovuto, o in violazione di legge/regolamento	Virus su PC ma che non trasmette dati su internet. Trasmissione non autorizzata di un documento non ancora validato dal suo autore.
Accesso non autorizzato	Un insieme di dati personali (e riconducibili all'interessato direttamente o indirettamente), a seguito di incidente o azione fraudolenta, sono stati resi disponibili per un intervallo di tempo a soggetti (anche se autorizzati dal Titolare ad altri trattamenti) non autorizzati ad accedere al dato secondo il principio di pertinenza e non eccedenza o in violazione di legge/regolamento	Deve trattarsi di dati appartenenti a documenti definitivi e già dotati di un livello minimo di validazione.	Accesso alla rete aziendale da esterni per vulnerabilità del sistema. Accesso da utenti a dati non di loro pertinenza a seguito di configurazione errata dei permessi di accesso al sistema.	Accesso da parte di utente a dati di sua pertinenza, al quale segue un uso improprio degli stessi. Accesso non autorizzato ad un documento non ancora validato da proprio autore.

TIPO DI DATA BREACH	DEFINIZIONE	ESTENSIONE MINIMA/SOGLIA DI SEGNALAZIONE	ESEMPI	ESEMPI DI CASI ESCLUSI
Indisponibilità temporanea del dato	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, rimane non disponibile per un periodo di tempo che lede i diritti dell'interessato.	Indisponibilità dei dati personali oltre i termini di tolleranza previsti e/o comunque correlati alla tipologia - finalità del dato.	Infezione da *ransomware* che comporta la temporanea perdita di disponibilità del dato, non ripristinabile dal back up. Cancellazione accidentale del dato da parte di persona non autorizzata. Perdita della chiave di decrittografia di dati crittografati..	Indisponibilità temporanea del dato causata da manutenzione programmata del sistema.