INDICE

MODIFICHE

Rev.	Data	Pagine modificate	Tipo/natura della modifica
0	19/09/2018		Prima emissione

SCOPO

Il presente documento ha lo scopo di indicare a tutto il personale operante presso l'Azienda USL di Modena le modalità di gestione di un *data breach*, ovvero di un episodio di violazione di dati personali, nel rispetto dei principi e delle disposizioni contenute nel Regolamento (UE) 679/2016 sulla protezione dei dati personali (GDPR).

In questo documento si sintetizzano le regole per garantire 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 del referente privacy
- valutazione dell'evento accaduto
- modalità e profili di segnalazione all'Autorità Garante
- eventuale comunicazione agli interessati

CAMPO DI APPLICAZIONE

La procedura si applica a tutto l'ambito aziendale e a tutti i soggetti che, a vario titolo, svolgano attività presso l'Azienda USL di Modena. La procedura si applica inoltre in presenza di possibili violazioni di dati personali, siano essi contenuti in banche informatiche o cartacee.

DEFINIZIONI

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, punto 1).

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, 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 (art. 4, punto 2).

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6).

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, sono titolari del trattamento le Aziende Sanitarie afferenti ad AVEN.

Referente privacy: la persona che all'interno della Azienda operativamente si occupa delle *policy* di privacy, propone la stesura dei relativi regolamenti ed effettua e valuta controlli sugli stessi.

Data Protection Officer (DPO): la persona individuata dal Titolare del trattamento (v. Delibera 110 del 27/04/2018) quale Responsabile della protezione dei dati personali, così come previsto per tutte le pubbliche amministrazioni dal GDPR.

Delegato al trattamento: la persona fisica che, secondo l'organizzazione aziendale, ricopre un ruolo gestionale e di responsabilità all'interno dell'azienda sanitaria che determina specifiche modalità organizzative rispetto ad uno o più trattamenti.

Autorizzato al trattamento: tutti i Direttori di Struttura Complessa e i Responsabili di Struttura Semplice Dipartimentale designati con Delibera 227 del 30/07/2018 (nonché taluni dirigenti espressamente individuati dal Titolare del trattamento), ai quali sono stati attribuiti specifici compiti e funzioni connessi al trattamento dei dati personali, sotto l'autorità del Titolare stesso.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

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.

DOCUMENTI DI RIFERIMENTO

- Regolamento (UE) 679/2016 sulla protezione dei dati personali (GDPR), considerando nn. 85, 86, 87, 88 e artt. 33, 34
- 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)
- D. Lgs. 196/2003 e s.m.i.
- Delibera N. 154 del 15/06/2018 – Regolamento (UE) N. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR) – ricognizione delle principali azioni di adeguamento della Azienda USL di Modena.

CONTENUTO

Premessa

Una violazione dei dati personali (c.d. *data breach*) 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.

Gestione del data breach interno alla struttura

Modalità e profili di notifica all'Autorità Garante Privacy

Ogni operatore aziendale autorizzato a trattare dati personali, qualora venga a conoscenza di un potenziale caso di *data breach,* avvisa tempestivamente il delegato al trattamento a cui afferisce (di norma il Direttore o il Responsabile della struttura presso cui presta servizio).

Il soggetto delegato a trattare i dati personali, valutato l'evento, se ritiene confermate le valutazioni di potenziale *data breach*, lo segnala tempestivamente inviando una mail al referente privacy, utilizzando il modulo allegato (All. 1), reperibile nella Sezione Privacy della Intranet Aziendale.

Home page intranet aziendale - sezione privacy

Il referente privacy effettua a sua volta una valutazione dell'evento avvalendosi, nel caso di eventuali altre professionalità necessarie per la corretta analisi della situazione del DPO per eventuali funzioni consulenziali.

Ai fini di una corretta classificazione dell'episodio, il referente privacy utilizzerà lo schema di scenario di *data breach*, allegato alla presente procedura.

Pertanto, sulla scorta delle determinazioni raggiunte e solo qualora ritenga che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, il referente privacy predispone l'eventuale notificazione all'Autorità Garante, a firma del Titolare del trattamento, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il Titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.

Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

E' comunque fatta salva la possibilità di fornire successivamente alla Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di *follow-up* (c.d. notifica in fasi).

La scelta e le motivazioni che hanno portato a non notificare l'evento devono essere documentate a cura del referente privacy.

Gestione del data breach esterno alla struttura

Ogniqualvolta l'Azienda/Titolare del trattamento 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 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*[1].

Modalità e profili di notifica all'Autorità Garante Privacy

Ogni responsabile del trattamento, qualora venga a conoscenza di un potenziale caso di *data breach* che riguardi dati di cui l'Azienda Usl di Modena sia Titolare, ne dà avviso senza ingiustificato ritardo alla Azienda stessa, inviando una mail al referente privacy e utilizzando il modulo (All.2) che ha ricevuto da parte della Azienda USL contestualmente al contratto di nomina.

Per "ingiustificato ritardo" si considera la notizia pervenuta al Titolare al più tardi entro 12 ore dalla presa di conoscenza iniziale da parte del responsabile.

Il referente privacy effettua a sua volta una valutazione dell'evento avvalendosi, nel caso, di eventuali altre professionalità necessarie per la corretta analisi della situazione del DPO per eventuali funzioni consulenziali.

Ai fini di una corretta classificazione dell'episodio il referente privacy utilizzerà lo schema di scenario di *data breach* allegato al presente schema di procedura.

Pertanto, sulla scorta delle determinazioni raggiunte e solo qualora ritenga che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, il referente privacy predispone l'eventuale notificazione all'Autorità Garante, a firma del titolare, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.

Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi)

La scelta e le motivazioni che hanno portato a non notificare l'evento devono essere documentate a cura del referente privacy.

Modalità di comunicazione agli interessati

Nel caso in cui dal *data breach* possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire

---

1

NB: Rimane salva la possibilità che sia il responsabile del trattamento ad effettuare una notifica per conto del titolare del trattamento, se il titolare del trattamento ha rilasciato specifica autorizzazione al responsabile, all'interno del suddetto contratto. Tale notifica deve essere fatta in conformità con gli articoli 33 e 34 del GDPR. La responsabilità legale della notifica rimane in capo al titolare del trattamento. In questa procedura si esamina solamente il caso d'uso ordinario in cui la notifica venga effettuata dal titolare del trattamento.

loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

Il referente privacy predispone l'eventuale comunicazione all'interessato/agli interessati, a firma del Titolare, da inviarsi nei tempi e nei modi che lo stesso, anche attraverso la funzione consulenziale del DPO, individuerà come più opportuna tenendo anche conto di eventuali indicazioni fornite dall'Autorità Garante. La comunicazione descriverà con un linguaggio semplice e chiaro la natura della violazione dei dati personali, le probabili conseguenze della stessa, nonché le misure individuate per porvi rimedio.

Registro delle violazioni

Presso l'Ufficio Privacy è istituito il registro delle violazioni, in cui sono documentati tutti gli episodi di *data breach* verificatisi dall'entrata in vigore del GDPR, e il cui aggiornamento è cura del referente privacy per conto del Titolare.

.

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 (non segnalare)
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	**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	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 (non segnalare)
	richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	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 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 fraudolenta, 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	Rientrano tra i casi di segnalazione i soli dati	Malfunzionamento del sistema di oscuramento del sistema	Il medico sul proprio sistema dipartimentale seleziona il

Tipo di Breach	Definizione	Estensione minima/Soglia di segnalazione	Esempi	Controesempi (non segnalare)
	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.	appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	dipartimentale che invia a SOLE Consegna di un CD con dati dei pazienti ad altra struttura senza autorizzazione	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.
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 autorizzato di un documento non ancora validato dal proprio autore.
Indisponibilità temporanea del	Un insieme di dati personali, a seguito di	Indisponibilità dei dati personali oltre i tempi	Infezione da *ransonware* che comporta la temporanea perdita di	Indisponibilità dei dati personali a causa della manutenzione

Tipo di Breach	Definizione	Estensione minima/Soglia di segnalazione	Esempi	Controesempi (non segnalare)
dato	incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato.	definiti a livello aziendale	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	programmata del sistema in corso

Un *data breach*, quindi, non è solo un attacco informatico, ma può consistere anche in un accesso abusivo, in 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, non idonei a identificare - in modo diretto o indiretto - l'interessato, non è considerato *data breach,* ma è considerato un normale errore procedurale (esempio: l'invio di un referto alla rete SOLE in cui il testo del referto è di un paziente mentre l'anagrafica è di un altro).

Questo poiché:

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

ALLEGATI

Allegato 1 DG.MO.009 "Modello per la segnalazione di un sospetto caso di data breach"
Allegato 2 DG.MO.010 "Segnalazione da parte di Ditta esterna di un sospetto caso di data breach"