



A.S.L. TO5

Regione Piemonte

*Azienda Sanitaria Locale
di Chieri, Carmagnola, Moncalieri e Nichelino*

*Sede Legale - Piazza Silvio Pellico n. 1 - 10023 Chieri (TO) - tel. 011 94291 - C.F. e P.I.
06827170017*

DELIBERAZIONE DEL DIRETTORE GENERALE

n. 72 del 25/01/2019

ADEMPIMENTI IN APPLICAZIONE DELL'ART. 33 DEL REGOLAMENTO GENERALE
PROTEZIONE DATI 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO -
APPROVAZIONE PROCEDURA IN CASO DI VIOLAZIONE DI DATI PERSONALI (DATA
BREACH)

Proponente - S.C. AFFARI GENERALI E PERSONALE -

Direttore - dott.ssa Caterina Burzio

Oggetto: ADEMPIMENTI IN APPLICAZIONE DELL'ART. 33 DEL REGOLAMENTO GENERALE PROTEZIONE DATI 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO - APPROVAZIONE PROCEDURA IN CASO DI VIOLAZIONE DI DATI PERSONALI (DATA BREACH)

IL DIRETTORE GENERALE
dott. Massimo Uberti

(nominato dalla Giunta Regionale con deliberazione n. 8-6927 del 29/05/2018)

Su proposta del Direttore della S.C. AFFARI GENERALI E PERSONALE, dott.ssa Caterina Burzio, che attesta la legittimità formale e sostanziale di quanto di seguito indicato nonché la regolarità della fase istruttoria espletata dal responsabile del procedimento di cui all'art. 5 della Legge 241/1990;

PREMESSO che

- il Regolamento (UE) 2016/679 del Parlamento e del Consiglio Europeo del 27 aprile 2016 disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali (in breve RGPD);
- l'art. 33 del suddetto RGPD 2016/679 così dispone: "In caso di violazioni di dati personali, il Titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 55, senza ingiustificato ritardo e, ove possibile, entro le 72 ore dal momento in cui ne 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. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo";
- le Linee Guida del Gruppo ex art. 29 n. 250 del 3 ottobre 2017, emendate in data 6 febbraio 2018, spiegano gli obblighi di notifica e di comunicazione in caso di violazioni dei dati personali, ai sensi del Regolamento EU 2016/679 e forniscono inoltre alcuni esempi di vari tipi di violazioni;

DATO atto che per "Data Breach" si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali" e cioè, nello specifico, 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 e che la mancata notifica può comportare ulteriori accertamenti da parte del Garante, poiché può rappresentare un indizio di carenze che, se accertate, possono dar luogo a sanzioni e, pertanto, tutti gli eventi di Data Breach, compresi quelli per cui la notifica non è necessaria, devono essere documentati in un "Registro delle Violazioni" (art. 33 paragrafo 5 RGPD);

RITENUTO necessario per quanto sin qui espresso adottare una procedura da porre in essere in caso di Data Breach che individui le azioni da porre in essere nel caso in cui venga accertata una violazione dei sistemi informatici, un'involontaria diffusione delle informazioni od altri eventi che rientrano nella definizione di "Data Breach";

RITENUTO altresì necessario individuare un Gruppo di Gestione Operativa Data Breach, che garantisca il pieno assolvimento degli obblighi previsti dalla normativa vigente in materia, con compiti e funzioni specificati nella procedura in oggetto;

CONSIDERATA l'importanza di individuare nel Gruppo due soggetti che fuori dell'orario di servizio, in reperibilità, siano preposti alla tempestiva ricezione, alla prima analisi delle segnalazioni e ai primi interventi di mitigazione, per evitare o limitare al minimo gli eventuali danni conseguenti alla violazione dei dati;

ACQUISITO il parere favorevole del Direttore Sanitario;

ACQUISITO il parere favorevole del Direttore Amministrativo;

D E L I B E R A

Per le motivazioni esposte in premessa:

1. di approvare la procedura da seguire in caso di violazione di dati personali "Data Breach", allegata alla presente deliberazione quale parte integrante e sostanziale;
2. di individuare il Gruppo di Gestione Operativa Data Breach così composto:

Direttore Generale o suo delegato
Direttore S.C. Sistemi Informativi e Tecnologie Integrate
Coordinatore del Gruppo Privacy
Dirigente Medico della Direzione Sanitaria (ricevente reperibile)
Direttore S.C. Approvvigionamenti e Logistica
Direttore S.C. Affari Generali e Personale
Direttore S.S. Qualità, Formazione e Accreditamento
Direttore S.S. Gestione del Patrimonio
Dirigente delle Professioni Sanitarie (Di.P.Sa.)
Responsabile del Gruppo Risk Management
Operatore Tecnico della S.C. Sistemi Informativi e Tecnologie Integrate (ricevente reperibile)
Responsabile della Gestione Documentale
Responsabile della Conservazione dei documenti digitale
Responsabile della Prevenzione della Corruzione e Trasparenza

3. di delegare il Coordinatore del Gruppo Privacy e, in sua assenza, il Direttore della S.C. Sistemi Informativi e Tecnologie Integrate, ad inoltrare la notifica al Garante di cui all'art. 33 del RGPD, nei casi in cui sarà necessaria;
4. dare mandato al Direttore della S.C. Sistemi Informativi e delle Tecnologie Integrate affinché sia portata a conoscenza di tutti i dipendenti e del personale assimilato la procedura in oggetto, tramite mail indirizzata alle caselle istituzionali aziendali e attraverso la pubblicazione del documento nell'Area Intranet del sito web aziendale;
5. di incaricare il Direttore della S.C. Sistemi Informativi e delle Tecnologie Integrate di programmare iniziative di formazione dirette ai soggetti che hanno competenze specifiche al fine di gestire gli eventi ed evitare o limitare i danni;
6. di comunicare il presente atto al Responsabile della Protezione dei Dati designato;
7. di dare atto che il presente provvedimento non comporta onere di spesa a carico del bilancio aziendale;
8. di dichiarare il presente provvedimento immediatamente esecutivo, ai sensi dell'art. 28 della Legge Regionale. 10 del 24/01/1995, ravvisata l'urgenza di provvedere per garantire la corretta gestione di eventuali violazioni di sicurezza.

Il Direttore Sanitario

- dott. Luciano Bernini -

Il Direttore Amministrativo
- dott. Massimo Corona –

Il Direttore Generale
- dott. Massimo Uberti -



A.S.L. TO5

Regione Piemonte

*Azienda Sanitaria Locale
di Chieri, Carmagnola, Moncalieri e Nichelino*

*Sede Legale - Piazza Silvio Pellico n. 1 - 10023 Chieri (TO) - tel. 011 94291 - C.F. e P.I.
06827170017*

DELIBERAZIONE DEL DIRETTORE GENERALE

n. 72 del 25/01/2019

ADEMPIMENTI IN APPLICAZIONE DELL'ART. 33 DEL REGOLAMENTO GENERALE
PROTEZIONE DATI 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO -
APPROVAZIONE PROCEDURA IN CASO DI VIOLAZIONE DI DATI PERSONALI (DATA
BREACH)

Publicata all'Albo Pretorio online dal 29/01/2019 al 07/02/2019

Esecutiva dal 25/01/2019



A.S.L. TO5

Regione Piemonte

*Azienda Sanitaria Locale
di Chieri, Carmagnola, Moncalieri e Nichelino*

*Sede Legale - Piazza Silvio Pellico n. 1 - 10023 Chieri (TO) - tel. 011 94291 - C.F. e P.I.
06827170017*

Questo atto è stato firmato digitalmente da:

Burzio Caterina - Direttore S.C. AFFARI GENERALI E PERSONALE

Petrucci Paolo - Direttore S.C. SISTEMI INFORMATIVI E TECNOLOGIE INTEGRATE

Bernini Luciano - Direttore Sanitario

Corona Massimo - Direttore Amministrativo

Uberti Massimo - Direttore Generale

Parodi Laura - il funzionario incaricato alla pubblicazione

PROCEDURA DA SEGUIRE IN CASO DI VIOLAZIONE DI DATI PERSONALI (DATA BREACH)

(ai sensi degli artt. 33 e 34 Regolamento UE 2016/679)

Sommario

1	RIFERIMENTI NORMATIVI.....	3
2	DEFINIZIONE DATA BREACH	4
3	PROCESSO DI NOTIFICAZIONE DATA BREACH.....	5
3.1	PIANIFICAZIONE.....	5
3.2	GESTIONE DELL'EVENTO.....	5
4	ACQUISIZIONE DELLA NOTIZIA	7
5	ANALISI TECNICA DELL'EVENTO.....	7
6	VALUTAZIONE DELLA GRAVITÀ DELL'EVENTO.....	8
7	NOTIFICA AL GARANTE DELLA PRIVACY	10
8	ALTRE SEGNALAZIONI DOVUTE.....	11
9	COMUNICAZIONE AGLI INTERESSATI.....	11
10	INSERIMENTO DELL'EVENTO NEL REGISTRO DELLE VIOLAZIONI	12
11	MIGLIORAMENTO	12
12	Allegato A – SOGGETTI PREPOSTI A GESTIRE LE VIOLAZIONI	13
13	Allegato B – MATRICE ASSEGNAZIONE RESPONSABILITÀ	14
14	Allegato C – MODELLO DI NOTIFICA DATA BREACH AL GARANTE PRIVACY	15

1 RIFERIMENTI NORMATIVI

- *Decreto Legislativo 10 agosto 2018 n. 101 “Disposizioni per l’adeguamento della Normativa Nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 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)”*
- *Regolamento (UE) 2016/679 del Parlamento Europeo del Consiglio del 27 aprile 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 – RGPD o, in inglese, GDPR): in particolare gli articoli 33 (Notifica all’Autorità di Controllo), 34 (notifica agli interessati) e 28 (Responsabile del trattamento)*
- *D.Lgs. 196/2003 “Codice per la protezione dei dati personali”*
- *Linee guida in materia di notifica delle violazioni di dati personali (Data Breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679*
- *Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche – Provvedimento Autorità Garante del 2 luglio 2015*
- *Provvedimento generale prescrittivo in tema di biometria – 12 novembre 2014*
- *ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary*
- *D.Lgs. 82/2005 “Codice dell’Amministrazione Digitale” (CAD)*
- *artt. 331 e 361 del Codice di Procedura Penale (obbligo di denuncia da parte del pubblico ufficiale)*
- *Decreto 9 gennaio 2008 del Ministero degli Interni in attuazione della Legge 155/2005 sulle infrastrutture critiche*
- *Decreto del Presidente del Consiglio dei Ministri 1 aprile 2008 “Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività” previste dall’articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell’amministrazione digitale» (G.U. 21 giugno 2008, n. 144)*
- *Art. 13 del Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014 “Definizione delle caratteristiche del sistema pubblico per la gestione dell’identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese. (14A09376) (G.U. 9 dicembre 2014, n. 285)*

2 DEFINIZIONE DATA BREACH

L'art. 33 del GDPR recita che: *“In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all’Autorità di controllo competente a norma dell’art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne 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. Qualora la notifica all’Autorità di controllo non sia effettuata entro 72 ore, è correData dei motivi del ritardo”*.

Per “Data Breach” si intende un evento in conseguenza del quale si verifica una “violazione dei dati personali”. Nello specifico, l’articolo 4 par. 1 punto 12 del GDPR definisce la violazione dei dati personali come *“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”*.

Le Linee guida in materia di notifica delle violazioni di dati personali (Data Breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679 precisano al p. I.B.2 quali sono i tipi di violazioni:

Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro ha spiegato che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni:

- *“violazione della riservatezza”, in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;*
- *“violazione dell’integrità”, in caso di modifica non autorizzata o accidentale dei dati personali;*
- *“violazione della disponibilità”, in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.*

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l’integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse. Ci si potrebbe chiedere se una perdita temporanea della disponibilità dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica. L’articolo 32 del regolamento (“Sicurezza del trattamento”) spiega che nell’attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, “la capacità di assicurare su base permanente la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento” e “la capacità di ripristinare tempestivamente la disponibilità e l’accesso dei dati personali in caso di incidente fisico o tecnico”.

Di conseguenza, un incidente di sicurezza che determina l’indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Va precisato che l’indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una “violazione della sicurezza” ai sensi dell’articolo 4, punto 12.

Come nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione), una violazione che implichi la perdita temporanea di disponibilità dovrebbe essere documentata in conformità all’articolo 33, paragrafo 5. Ciò aiuta il titolare del trattamento a dimostrare l’assunzione di responsabilità all’autorità di controllo, che potrebbe chiedere di consultare tali registrazioni. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all’autorità di controllo e la comunicazione alle persone fisiche coinvolte. Il titolare del trattamento dovrà valutare la probabilità e la gravità dell’impatto dell’indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche. Conformemente all’articolo 33, il titolare del trattamento dovrà effettuare la notifica a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Questo punto dovrà chiaramente essere valutato caso per caso.

Va notato che, sebbene una perdita di disponibilità dei sistemi del titolare del trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il titolare del trattamento consideri tutte le possibili conseguenze della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi.

La mancata notifica può comportare ulteriori accertamenti da parte del Garante poiché può rappresentare un indizio di carenze che, se accertate, possono dar luogo a sanzioni.

Tutti gli eventi di Data Breach, compresi quelli per cui non sono necessarie le notifiche, devono essere documentati (art. 33 par. 5 del GDPR) su un Registro delle Violazioni.

3 PROCESSO DI NOTIFICAZIONE DATA BREACH

Prima che si verifichi un incidente di sicurezza occorre predisporre le procedure, gli strumenti e l'organizzazione per gestire l'evento fortuito al meglio.

Una finalità della procedura è quella di porre una particolare attenzione perché siano effettuati tutti gli sforzi per evitare o limitare i danni (c.d. resilienza richiesta dalla norma), e consentire che siano rispettati i tempi molto brevi richiesti per la segnalazione al Garante, indicati nell'art. 4

3.1 PIANIFICAZIONE

Saranno programmate iniziative di formazione e informazione a tutto il personale affinché sia messo in condizione di segnalare per tempo gli eventi che comportano un Data Breach, e soprattutto abbia coscienza della necessità ed importanza di far pervenire i dati necessari in tempi brevissimo.

Alcuni servizi avranno una formazione particolare (S.S. Gestione del Patrimonio per i furti, Direzioni Sanitarie per cartelle cliniche, Sistemi Informativi e Ingegneria Clinica, Tecnico e URP per altri eventi), per individuare gli eventi e raccogliere le informazioni necessarie e poi inoltrarle ai Riceventi dell'allegato A.

I soggetti individuati nell'allegato A come Soggetti Competenti devono, nell'ambito delle loro competenze:

- predisporre i mezzi e gli strumenti tecnologici ed organizzativi per:
 - Individuare
 - Analizzare
 - Risponderealle potenziali violazioni dei dati, anche coinvolgendo i fornitori;
- predisporre apposite clausole contrattuali con i fornitori Responsabili del Trattamento per la miglior gestione degli incidenti di sicurezza e delle violazioni;
- fornire consulenza specialistica nel settore di competenza in supporto ai soggetti Riceventi.

3.2 GESTIONE DELL'EVENTO

In caso di accertamento di incidente, sarà opportuno seguire i seguenti steps del processo di notificazione:

1. Acquisizione della notizia da parte dei soggetti Riceventi (individuati nell'allegato A) che provvederanno ad attivare i passi successivi;

2. Analisi tecnica dell'evento per determinare se vi è stata violazione
3. Contenimento del danno;
4. Valutazione della gravità dell'evento;
5. Notifica al Garante Privacy;
6. Altre segnalazioni dovute;
7. Comunicazione agli interessati, ove necessaria;
8. Inserimento dell'evento nel Registro delle Violazioni;
9. Azioni correttive specifiche e per analogia.

4 ACQUISIZIONE DELLA NOTIZIA

La segnalazione di un Data Breach può essere interna o esterna all'Ente.

- INTERNAMENTE:
 1. da personale dipendente
 2. da personale convenzionato/stagisti/tirocinanti, ecc.
- ESTERNAMENTE
 1. da parte degli organi Pubblici (Agid, Polizia, altre Forze dell'Ordine, giornalisti, ecc.)
 2. da parte del DPO
 3. da parte dei Responsabili esterni del trattamento
 4. da parte degli interessati
 5. da parte di ulteriori soggetti.

La segnalazione deve essere inoltrata ai soggetti preposti individuati nell'allegato A quali **Riceventi** mediante:

- posta elettronica;
- avvertimento verbale/telefonico in ogni caso.

Dal momento in cui i soggetti preposti predetti, vengono a conoscenza dell'evento, decorre il termine delle 72 ore previsto dalla normativa per l'invio della notifica all'Autorità di controllo.

Tale termine è ridotto a 48 ore nel caso in cui i trattamenti oggetto dell'evento rientrino in quelli previsti dalle misure di sicurezza e modalità di scambio dei dati personali tra Amministrazioni Pubbliche – provvedimento n. 393 del 2 luglio 2015 (Pubblicato sulla Gazzetta Ufficiale n. 179 del 4 agosto 2015).

Per le violazioni di dati biometrici il termine, come indicato dal Garante nel provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014, è di 24 ore.

5 ANALISI TECNICA DELL'EVENTO

Nella fase iniziale si distinguono due procedure:

- a) fuori normale orario di servizio (notturno, festivo)
- b) in orario di servizio

a) Si prevede infatti che la segnalazione possa pervenire in qualsiasi orario, e vista l'importanza della tempestività delle azioni, nel caso di evento e/o segnalazione fuori orario di servizio siano attivati i Riceventi reperibili (v. allegato A).

I Riceventi reperibili, dopo una analisi preliminare, attuano le prime azioni per il contenimento delle conseguenze (es. mettono sotto chiave la cartella cartacea lasciata fuori posto o spengono il dispositivo elettronico guasto e chiamano l'assistenza di secondo livello).

b) Dopo la prima messa in sicurezza, le successive azioni saranno svolte in orario di servizio seguendo la procedura di cui al punto b) I Riceventi in normale orario di servizio, dopo un'analisi preliminare, attivano il Gruppo di Gestione (v. allegato A), sotto la supervisione del Coordinatore del Gruppo Privacy. Il Gruppo che gestisce gli incidenti, è responsabile, sulla base delle rispettive competenze, in base alla tipologia dell'incidente, dell'analisi tecnica dell'evento, delle azioni da mettere in atto

tempestivamente per il contenimento o annullamento del danno, avvalendosi della collaborazione delle figure indicate nella tabella “assegnazione responsabilità” (allegato B).

In particolare, una volta verificato che l’evento segnalato si configuri effettivamente come un “Data Breach” (Analisi Preliminare), e solo dopo aver attivato tutte le azioni di contenimento possibili, verranno svolte tutte le operazioni necessarie a raccogliere gli elementi per una valutazione dell’evento (Analisi Approfondita) ai fini della notifica al Garante della Privacy. È importante sottolineare che, anche nel caso in cui dall’Analisi Preliminare emerga che la segnalazione non ha i caratteri del Data Breach, è necessario registrarla nel Registro delle Violazioni.

Durante l’Analisi Approfondita, dovranno essere accertate le circostanze della violazione, le conseguenze e i relativi rimedi.

Si precisa che l’art. 33 paragrafo n. 4 del DGPR recita “*Qualora nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo*”. Pertanto, sarà fondamentale raccogliere il maggior numero di informazioni e, anche in caso queste non siano per il momento ritenute esaustive, effettuare la notificazione.

Nello specifico verrà effettuato, in un tempo consigliabile non superiore a 8 – 10 ore:

- il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità) o altro evento (cfr Linee Guida sulla notifica delle Violazioni dei dati personali ai sensi del Regolamento UE 2016/79 WP 250 par. 1 punto 2)
- l’identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
- l’identificazione degli interessati;
- il contenimento del danno come di seguito descritto:
 - limitazione o annullamento degli effetti dell’incidente,
 - raccolta delle prove forensi nel caso sia ipotizzato un reato,
 - determinazione delle azioni possibili di ripristino, e avvio delle stesse
 - ripristino dei dati, dei sistemi, dell’infrastruttura e delle configurazioni,
 - valutazione dei tempi di ripristino,
 - gestione della comunicazione con i Clienti, con CERT-PA/Polizia Postale e con i media,
 - verifica dei sistemi recuperati.
 - valutazione delle eventuali vulnerabilità collegate con l’incidente,
 - individuazione delle azioni di mitigazione delle vulnerabilità individuate,

Tutte le operazioni effettuate devono essere tracciate e riconducibili a specifiche persone, sulla base dell’allegato B.

6 VALUTAZIONE DELLA GRAVITÀ DELL’EVENTO

Il Direttore della S.C. Sistemi Informativi e Tecnologie Integrate e il Coordinatore del Gruppo Privacy, con il supporto dei soggetti competenti, dovranno appurare se l’evento merita di essere notificato al Garante della Privacy e con quali modalità (notifica unica o per fasi).

Insieme ai soggetti interni di ausilio alla fase di analisi tecnica, si dovrà:

- informare tempestivamente il RPD;
- accertare la probabilità o meno che l’evento abbia comportato dei rischi per i diritti e la libertà delle persone (cioè quando si è verificato una distruzione,

perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati, sia che questi dati siano trattati all'interno che all'esterno);

- effettuare la notifica al Garante, se necessaria;
- verificare, successivamente, se sia necessaria una seconda notifica più approfondita, di conseguenza ad una analisi tecnica supplementare;
- effettuare una comunicazione all'Autorità giudiziaria competente, se necessaria e se non ancora effettuata dai Riceventi nelle prime fasi.

L'art. 33 paragrafo n. 1 chiarisce che non vi è obbligo di notifica della violazione quando è "improbabile" che questa comporti un rischio per i diritti e le libertà delle persone fisiche, ovviamente il giudizio che determina l'improbabilità del rischio deve essere riportato nel Registro delle Violazioni.

A questo proposito, i Garanti europei nelle loro linee guida, precisano che la mancata comunicazione può essere sanzionata ma che nessuna sanzione è prevista nel caso di comunicazione incompleta o di comunicazione non necessaria.

Nella fase di Valutazione, sulla base delle informazioni predisposte in fase di Pianificazione, occorre innanzitutto stabilire se nell'incidente sono coinvolti i dati personali. In caso di risposta positiva occorre valutare l'impatto sugli interessati. Se si tratta di una violazione di riservatezza occorre verificare che le misure di sicurezza (es.: cifratura dei dati) in vigore rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note). In caso di perdita di integrità o disponibilità di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati.

Se in tale modo i rischi per gli interessati sono trascurabili, la procedura può terminare, dopo aver documentato il processo e le scelte operate: le misure messe in atto sono state adeguate alla minaccia. La fase di Miglioramento può essere innescata per incrementare ulteriormente la protezione del dato, ma non è obbligatoria.

Nel caso che i rischi per l'interessato non siano trascurabili occorre procedere come di seguito:

1. si ha il dovere di notificare al Garante, questo può presentarsi in 3 sottocasi:
 - a. l'organizzazione è Titolare del/i trattamenti dei dati coinvolti nell'incidente
 - b. l'organizzazione è Contitolare del trattamento con delega alla notifica
 - c. l'organizzazione è Responsabile del trattamento con delega alla notifica.
2. L'organizzazione non ha nemmeno potenzialmente il dovere di notificare all'Autorità Garante: questo quando l'ASL TO5 agisce come Responsabile del trattamento per conto di altro Titolare, senza delega alla notifica al Garante.

Nella seconda ipotesi l'organizzazione deve comunicare al Titolare la sospetta violazione e/o l'incidente di sicurezza riguardante dati personali al Titolare stesso nei modi convenuti con la massima tempestività e mettersi a disposizione di quest'ultimo per approfondimenti e contenimento dei danni.

Nella prima ipotesi occorre valutare, seguendo le indicazioni dei documenti sopracitati, se il rischio per gli interessati è probabile. In questa fase come prima indicazione occorre assumere come rischio il massimo risultante dall'analisi fatta in fase di Pianificazione. L'analisi del caso specifico deve portare ad una valutazione specifica. L'analisi dei rischi per gli interessati deve dare le giuste priorità agli sforzi di contenimento dell'incidente, nonché fare proseguire la procedura nel caso in cui la soglia sia superata. In ogni caso va condotta la fase di Miglioramento.

Qualora i contorni della compromissione non siano chiari si può attendere fino ad un massimo di 72 ore prima di effettuare una notifica. Alla scadenza delle 72 ore è opportuno fare una comunicazione significando che questa è l'inizio di una notifica in fasi. Si può valutare di fare una notifica cumulativa se una stessa compromissione ha riguardato la stessa tipologia di dati con le stesse modalità.

Per completare la comunicazione, se temporalmente fattibile, occorre individuare:

- le misure di contenimento adottate
- il numero anche approssimativo di interessati
- il periodo di violazione
- se si ritiene di informare o meno gli interessati e le relative motivazioni
- le misure di contenimento del danno da suggerire agli interessati
- il carattere transfrontaliero e la nazionalità degli interessati o meno
- le azioni di miglioramento intraprese.

7 NOTIFICA AL GARANTE DELLA PRIVACY

Come accennato, la notifica di una violazione al Garante è resa obbligatoria dall'art. 33 del GDPR nei casi in cui si verifichi una violazione dei dati personali, a meno che sia improbabile che tale violazione presenti un rischio per i diritti e le libertà delle persone fisiche.

La notifica è effettuata su delega del Titolare dal Coordinatore del Gruppo Privacy o in sua assenza, dal Direttore della S.C. Sistemi Informativi e Tecnologie Integrate, sulla base del Modello reso disponibile dal Garante della privacy (allegato C) e dovrà contenere i seguenti elementi:

- la descrizione della violazione dei dati personali compresi, ove possibile le categorie e il numero approssimativo di interessati in questione nonché le categorie ed il numero approssimativo di registrazioni dei dati personali in questione;
- l'indicazione del nome ed i relativi dati di contatto del RPD;
- la descrizione delle probabili conseguenze della violazione;
- l'indicazione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e che, se del caso, per attenuare i possibili effetti negativi;
- nello specifico, la notifica al Garante sarà effettuata tramite PEC e per conoscenza al RPD, con indicazione del RPD come punto di contatto con il Garante.

Se l'estensione della compromissione è chiara e non si sono verificati episodi analoghi si deve procedere alla notifica all'Autorità.

I contenuti della notifica sono specificati dal GDPR e dai documenti citati.

8 ALTRE SEGNALAZIONI DOVUTE.

Il Coordinatore del Gruppo Privacy, con il supporto dei soggetti Competenti, dovrà verificare la necessità di informare altri organi quali:

- CERT-PA (in caso di incidenti informatici ai sensi della Circolare Agid n. 2/2017 del 18.04.2017);
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti), tra cui la Polizia Postale e delle comunicazioni;
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche).
- al Gestore di Identità Digitale e ad Agid nel caso in cui si individui un uso anomalo di un'identità SPID (Sistema Pubblico di Identità Digitale).

9 COMUNICAZIONE AGLI INTERESSATI

In caso di elevato rischio per la libertà e i diritti degli individui, si provvederà ad informare gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio.

La comunicazione agli interessati, secondo quanto previsto dal paragrafo n. 3 dell'art. 34 del GDPR, non è richiesta quando:

- 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;
- 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 di cui al paragrafo 1;
- la comunicazione richiederebbe sforzi sproporzionati.

In tal caso, si procede invece ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

La comunicazione deve contenere, ai sensi dell'art. 34, le seguenti informazioni:

- il nome e i dati di contatto del RPD o di altro punto di contatto;
- la descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

A valle della decisione di notificare l'Autorità Garante, occorre valutare se è il caso di notificare anche gli interessati. A tale scopo va valutata la gravità del rischio per gli interessati e i loro diritti.

Se il rischio è grave occorre individuare:

- la fattibilità di contattarli singolarmente oppure la necessità di procedere con pubblicazioni su diversi mezzi di comunicazione (sito web, quotidiani, radio, tv)
- le misure di contenimento che gli stessi interessati possano mettere in atto per minimizzare i rischi
- le forme di comunicazione più comprensibili per gli interessati (mezzi, lingue, linguaggio) come indicato nelle Linee guida elaborate dal Gruppo Art. 29 in materia di trasparenza (WP 260), definite in base alle previsioni del Regolamento (UE) 2016/679.

Anche di queste fasi deve essere prodotta e conservata appropriata documentazione.

L'attività descritta in questo punto 9 viene svolta sotto la responsabilità del Direttore della S.C. Sistemi Informativi e Tecnologie Integrate e del Coordinatore del Gruppo Privacy, previa informazione del Titolare del trattamento dati nella persona del Direttore Generale, che coinvolgerà a seconda dei casi, i Direttori di Struttura interessati negli incidenti e/o l'Ufficio Stampa aziendale.

10 INSERIMENTO DELL'EVENTO NEL REGISTRO DELLE VIOLAZIONI

L'art. 33 paragrafo n. 5 del DGPR, prescrive al Titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.

Pertanto, il Coordinatore del Gruppo Privacy dovrà inserire nel registro delle violazioni l'evento che sarà documentato e tracciabile e in grado di fornire evidenza nelle sedi competenti.

Per quanto riguarda la documentazione delle violazioni, Il Titolare del trattamento tiene conto del parere del RPD in merito alla struttura, all'impostazione e all'amministrazione della documentazione stessa.

11 MIGLIORAMENTO

Le azioni di miglioramento previste in fase di applicazione della presente procedura sono le seguenti:

- analisi dell'incidente con figure tecniche-professionali competenti per individuare le vulnerabilità;
- adozione di nuovi sistemi tecnici di prevenzione/protezione e/o di sistemi di controllo/monitoraggio/allarme;
- individuazione di controlli e misure di sicurezza che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
- valutazione su possibilità di copertura assicurativa;
- azioni informative rivolte ai dipendenti;
- revisione delle relazioni con Clienti e Fornitori;
- pianificare dei test periodici per verificare la validità della presente procedura;
- revisione della procedura, se necessaria, e di eventuali altri documenti collegati.

Tali azioni verranno definite dal Titolare o suo delegato.

12 ADEMPIMENTI

Tale procedura sarà diffusa a tutti i soggetti deputati al trattamento dei dati personali che, a diverso titolo, potranno e dovranno essere di ausilio al Titolare del trattamento, tramite la pubblicazione nell'Area Intranet del sito web aziendale.

Inoltre verranno predisposte azioni informative di cui si darà conoscenza attraverso mail inviate agli indirizzi istituzionali dei dipendenti e del personale assimilato

Allegato A – SOGGETTI PREPOSTI A GESTIRE LE VIOLAZIONI

Gruppo Gestione Operativa Data Breach

Ruoli	Riceventi reperibili	Riceventi	Competenti
Titolare del trattamento nella persona del Direttore Generale		Si	
Direttore S.C Sistemi Informativi e Tecnologie Integrate		Si	Si
Coordinatore del Gruppo Privacy		Si	
Dirigente Medico della Direzione Sanitaria	SI		
Operatore Tecnico della S.C. Sistemi Informativi e Tecnologie Integrate	SI		
Responsabile della Gestione Documentale			Si
Responsabile della Conservazione dei documenti digitale			Si
Dirigente delle Professioni Sanitarie (Di.P.Sa)			Si
Responsabile Ingegneria Clinica			Si
Responsabile del Gruppo Risk Management			Si
Responsabile della Prevenzione della Corruzione e Trasparenza			Si
Direttore S.C. Approvvigionamenti e Logistica			Si
Direttore S.C. Affari Generali e Personale			Si
Direttore S.S. Qualità, Formazione e Accreditamento			Si
Responsabile Ufficio Comunicazione e Relazione con il Pubblico			Si
Direttore S. S. Gestione del Patrimonio			Si

Riceventi reperibili	Preposti alla ricezione, prima analisi delle segnalazioni e primi interventi di mitigazione, fuori orario di servizio
Riceventi	Preposti alla ricezione, alla prima analisi delle segnalazioni e comunicazione in orario di servizio
Competenti	Predispongono mezzi e strumenti, forniscono consulenza specialistica per le violazioni nell'ambito del dominio di competenza

Allegato B - ASSEGNAZIONE RESPONSABILITÀ

Step (art.3)	Segnalante interno	Riceventi reperibili	Direttore della S.C. Sistemi Informativi e Tecnologie Integrate	Competenti	Coordinatore Gruppo Privacy	RPD	Titolare del trattamento nella persona del Direttore Generale
Rilevazione incidente	R	I	A		A		I
Acquisizione della notizia		R	R		A		I
Analisi tecnica dell'evento	C	R	R	R	A	C	I
Contenimento del danno	C	R	R	R	A	C	I
Valutazione della gravità dell'evento	C		R	C	R	C	A (evento significativo)
Notifica al Garante Privacy			R	C	R	C	A
Altre segnalazioni dovute ¹	R		R	C	R	C	A (evento significativo)
Comunicazione agli interessati			R	C	R	C	A (evento significativo)
Inserimento dell'evento nel Registro delle Violazioni			I	R	R	I	I
Azioni correttive			R	R	C	C	A

Legenda

- R** Responsabile dell'attività
- A** Approva e supervisiona
- C** Consultato
- I** Informato

I soggetti competenti sulla tipologia della segnalazione possono/debbono avvalersi delle Ditte appaltatrici per il necessario supporto.

¹ Le altre segnalazioni sono effettuate secondo le deleghe in essere

Allegato C – MODELLO DI NOTIFICA DATA BREACH AL GARANTE PRIVACY

1. Titolare che effettua la comunicazione:
 - a. Denominazione o ragione sociale
 - b. Sede del Titolare
 - c. Persona fisica addetta alla comunicazione
 - d. Funzione rivestita
 - e. Indirizzo e-mail per eventuali comunicazioni
 - f. Recapito telefonico per eventuali comunicazioni

2. Natura della comunicazione:
 - a. Nuova comunicazione (inserire contatti per eventuali chiarimenti, se diversi da quelli sub 1.)
 - b. Seguito di precedente comunicazione (inserire numero di riferimento)
 - b1. Inserimento ulteriori informazioni sulla precedente comunicazione
 - b2. Ritiro precedente comunicazione (inserire le ragioni del ritiro)

3. Denominazione della/e banca/banche dati oggetto di Data Breach e breve descrizione della violazione di dati personali ivi trattati.

4. Quando si è verificata la violazione di dati personali?
 - a. il.....
 - b. tra il.....e il.....
 - c. in un tempo non ancora determinato
 - d. È possibile che sia ancora in corso

5. Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smaltimento di dispositivi o di supporti portatili).

6. Modalità di esposizione al rischio:
 - a. tipo di violazione:
 - a.1. lettura (presumibilmente i dati non sono stati copiati)
 - a.2. copia (i dati sono ancora presenti sui sistemi del Titolare)
 - a.3. alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
 - a.4. cancellazione (i dati non sono più sui sistemi del Titolare e non li ha neppure l'autore della violazione)
 - a.5. furto (i dati non sono più sul sistema del Titolare e li ha l'autore della violazione)
 - a.6. altro (specificare)

 - b. dispositivo oggetto della violazione:
 - b.1. computer
 - b.2. dispositivo mobile
 - b.3. documento cartaceo
 - b.4. file o parte di un file
 - b.5. strumento di backup
 - b.6. rete

b.7. altro (specificare)

7. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.
8. Quante persone sono state colpite dalla violazione di dati personali?
 - a. (numero esatto) persone
 - b. circa (numero) persone
 - c. un numero (ancora) sconosciuto di persone
9. Che tipo di dati sono coinvolti nella violazione?
 - a. Dati anagrafici
 - b. Numeri di telefono
 - c. Indirizzi di posta elettronica
 - d. Dati di accesso e di identificazione (username, password, customer ID, altro)
 - f. Altri dati personali (sesso, Data di nascita/età,...) dati sensibili e giudiziari
 - g. Ancora sconosciuto
 - h. Altro (specificare)
10. Livello di gravità della violazione di dati personali (secondo le valutazioni del Titolare):
 - a. Basso/trascurabile
 - b. Medio
 - c. Alto
 - d. Molto alto
11. Misure tecniche e organizzative applicate ai dati colpiti dalla violazione.
12. La violazione è stata comunicata anche a contraenti (o ad altre persone interessate)?
 - a. Sì, e stata comunicate il.....
 - b. No, perché (specificare)

13. Qual'è il contenuto della comunicazione ai contraenti (o alle persone interessate)?(riportare il testo della comunicazione)
14. Quale canale è utilizzato per la comunicazione ai contraenti (o alle altre persone interessate)?
15. Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?
16. La violazione coinvolge contraenti (o altre persone interessate) che si trovano in altri Paesi EU?
17. La comunicazione è stata effettuata alle competenti Autorità di altri Paesi EU?
 - a. No
 - b. Sì (specificare)