REGOLAMENTO AZIENDALE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
AZIENDA SANITARIA LOCALE BT

Relativo al cd. *Data Breach*.

Ufficio DPO/RPD Avv. Andrea Scarpellini Camilli

andrea.scarpellini@aslbat.it;

dpo@mailcert.aslbat.it

Tel. 0883.299.466

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.

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), 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 - 2 luglio 2015
- D.Lgs. 82/2005 Codice dell'Amministrazione Digitale (CAD)

Ufficio DPO/RPD Avv. Andrea Scarpellini Camilli
andrea.scarpellini@aslbat.it;
dpo@mailcert.aslbat.it
Tel. 0883.299.466

- 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 DPCM 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), nonchè dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese. (14A09376) (GU Serie Generale n.285 del 09-12-2014)

PREMESSO ANCORA

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 p.12 del GPDR 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

Ufficio DPO/RPD Avv. Andrea Scarpellini Camilli
andrea.scarpellini@aslbat.it;
dpo@mailcert.aslbat.it
Tel. 0883.299.466

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 la nozione di violazione come di seguito riportata:
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 informazioni14:

- "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, accesso15 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

Ufficio DPO/RPD Avv. Andrea Scarpellini Camilli
andrea.scarpellini@aslbat.it;
dpo@mailcert.aslbat.it
Tel. 0883.299.466

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 registrazioni16. 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.

Ufficio DPO/RPD Avv. Andrea Scarpellini Camilli

andrea.scarpellini@aslbat.it;

dpo@mailcert.aslbat.it

Tel. 0883.299.466

1 Scopo del documento e ambito di applicazione

Il presente documento si prefigge lo scopo di indicare agli operatori della Asl BT 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 UE 679/2016.

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
- modalità e profili di segnalazione all'Autorità Garante
- valutazione dell'evento accaduto
- eventuale comunicazione agli interessati

2 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.

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.

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo

Ufficio DPO/RPD Avv. Andrea Scarpellini Camilli
andrea.scarpellini@aslbat.it;
dpo@mailcert.aslbat.it
Tel. 0883.299.466

criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

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 la Azienda Sanitaria Locale BAT.

Responsabile privacy: laddove previsto è la persona fisica che operativamente si occupa delle *policy* di privacy, propone la stesura dei regolamenti sulla privacy e sul trattamento dati ed effettua e valuta controlli sugli stessi. Nelle aziende è talvolta chiamato "coordinatore privacy" e, come collocazione ottimale, dovrebbe essere inserito come Direttore di U.O.S. all'interno della SBL.

Data Protection Officer: altrimenti detto **Responsabile Protezione Dati**, la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).

Designato / Incaricato (già Responsabile) del 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: la persona fisica, espressamente delegata, che opera sotto l'autorità del titolare del trattamento o del suo delegato/incaricato, con specifici compiti e funzioni connessi al trattamento

Ufficio DPO/RPD Avv. Andrea Scarpellini Camilli

andrea.scarpellini@aslbat.it;

dpo@mailcert.aslbat.it

Tel. 0883.299.466

dei dati personali.

Responsabile (esterno) 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.

3 Gestione del *data breach* interno alla struttura

Premesse

È necessario che l'azienda sanitaria dia notizia a tutti gli operatori in merito alla presente procedura mediante idonea delibera e circolare.
Nell'Azienda verrà individuato il responsabile dell'Ufficio Privacy, laddove possibile, ed è opportuno che sia affiancato all'interno di una U.O.S. da un gruppo privacy (gruppo multidisciplinare di professionisti che supportano il RPD per specificità tecniche).
Il Responsabile dell'Ufficio Privacy assumerà, ai fini della presente procedura, il ruolo di responsabile del processo e sarà sostituito dal RPD/DPO nell'eventualità il suolo non fosse individuato ed assegnato.

Modalità e profili di notifica all'Autorità Garante Privacy

Ogni operatore aziendale autorizzato a trattare dati, qualora venga a conoscenza di un potenziale caso di *data breach,* avvisa tempestivamente il diretto superiore.
Quest'ultimo, valutato l'evento, se confermate le valutazioni di potenziale *data breach*, lo segnala tempestivamente al RPD/DPO anche per le vie brevi, seguite da comunicazione scritta dettagliata.
La segnalazione perviene al RPD/DPO tramite le consuete modalità di gestione dei flussi documentali già in uso.

Ufficio DPO/RPD Avv. Andrea Scarpellini Camilli
andrea.scarpellini@aslbat.it;
dpo@mailcert.aslbat.it
Tel. 0883.299.466

Il responsabile privacy (qualora previsto) effettua una valutazione dell'evento con il RPD/DPO, in mancanza la detta valutazione sarà compiuta dal solo RPD/DPO.

Sulla scorta delle determinazioni raggiunte, il RPD/DPO si accerta che venga predisposta l'eventuale comunicazione 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 dovrà essere corredata delle ragioni del ritardo. È 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 deve essere documentata a cura del titolare.

4 Gestione del *data breach* esterno alla struttura

Premesse

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*.

Ad ogni responsabile del trattamento deve essere comunicato il contatto del RPD/DPO al quale effettuare la predetta segnalazione.

Modalità e profili di notifica all'Autorità Garante Privacy

Ogni designato al trattamento, qualora venga a conoscenza di un potenziale

Ufficio DPO/RPD Avv. Andrea Scarpellini Camilli
andrea.scarpellini@aslbat.it;
dpo@mailcert.aslbat.it
Tel. 0883.299.466

data breach che riguardi dati di cui l'azienda sia titolare, ne dà avviso senza ingiustificato ritardo al RPD/DPO.

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 responsabile privacy, ove previsto, effettua una valutazione dell'evento di concerto con il del RPD/DPO. Pertanto, sulla scorta delle determinazioni raggiunte, il referente privacy, di concerto con il del RPD/DPO, predispone l'eventuale comunicazione 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 dovrà essere corredata delle ragioni del ritardo.

È 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 deve essere documentata a cura del referente privacy.

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

Il responsabile privacy (ovvero il del RPD/DPO) 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 del del RPD/DPO, individuerà come più opportuna come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

Un *data breach* non è solo un attacco informatico, ma può consistere anche in

Ufficio DPO/RPD Avv. Andrea Scarpellini Camilli
andrea.scarpellini@aslbat.it;
dpo@mailcert.aslbat.it
Tel. 0883.299.466

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* 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 né posso essere ricondotti al reale 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.

6 Registro delle violazioni

Il responsabile privacy, ove previsto, cura l'aggiornamento del registro delle violazioni, ai sensi dell'art. 33, comma 5 del GDPR, obbligo che resta in capo al Titolare.

8 Norma di rinvio

Per quanto non espressamente disciplinato dal presente Regolamento si rimanda al Regolamento UE 2016/679 nonchè quanto previsto dal D. Lgs. 196/03 e successive modificazioni ed integrazioni.

Si propone per l'approvazione in data 19.07.2019

Ufficio DPO/RPD Avv. Andrea Scarpellini Camilli

andrea.scarpellini@aslbat.it;

dpo@mailcert.aslbat.it

Tel. 0883.299.466

Allegato A – MODELLO DI NOTIFICA DATA BREACH AL GARANTE.

1. Indicazione dei dati del 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
g. Identificazione del RPD/DPO e dati di contatto

2. Natura della comunicazione:
a. Nuova comunicazione (inserire contatti per eventuali chiarimenti)
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)

Ufficio DPO/RPD Avv. Andrea Scarpellini Camilli
andrea.scarpellini@aslbat.it;
dpo@mailcert.aslbat.it
Tel. 0883.299.466

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)

Ufficio DPO/RPD Avv. Andrea Scarpellini Camilli

andrea.scarpellini@aslbat.it;

dpo@mailcert.aslbat.it

Tel. 0883.299.466

Data e Firma

Ufficio DPO/RPD Avv. Andrea Scarpellini Camilli

andrea.scarpellini@aslbat.it;

dpo@mailcert.aslbat.it

Tel. 0883.299.466