ASL Taranto

REGOLAMENTO AZIENDALE
PER LA GESTIONE DEI DATA BREACH

Versione 1.0
28 dicembre 2018

Sommario

Cos'è la violazione dei dati personali (Data Breach)

La sezione 2 del Regolamento Europeo 2016/679 (GDPR) (artt. 32 – 34) si occupa della gestione della sicurezza dei dati personali.
Per Violazione di dati s'intende "*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*" (art. 4 p. 12 GDPR).
Si ha distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento. Si ha un danno quando i dati personali sono stati modificati, corrotti o non sono più completi. La perdita dei dati personali si verifica allorquando i dati, pur continuando ad esistere, non sono più nel controllo o nel possesso del titolare. Infine, un trattamento non autorizzato o illecito può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati, oppure qualsiasi altra forma di trattamento in violazione del regolamento.
Possiamo distinguere una violazione (Breach) da un mero Incidente (Incident) dalla conferma della divulgazione dei dati rispetto ad una potenziale esposizione a terzi non autorizzati.
Una violazione può avere potenzialmente numerosi effetti negativi significativi sulle persone fisiche, che possono causare danni fisici (si pensi, ad esempio, ad una non corretta refertazione di un esame diagnostico che può portare alla prescrizione di una cura errata per un paziente), materiali o immateriali: ad esempio la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo alle persone fisiche interessate.
La violazione dei dati è un particolare tipo di incidente di sicurezza grazie al quale il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali (sicurezza, legittima finalità del trattamento, limitatezza, correttezza, etc.).
È dunque necessario che il titolare possa identificare gli eventuali incidenti che possano verificarsi ed individuare contestualmente l'impatto che tali accadimenti hanno sui dati e in particolare sui dati personali trattati.
Il GDPR impone tanto al titolare quanto al responsabile del trattamento di disporre di misure tecniche e organizzative che garantiscano un adeguato livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati. Essi dovrebbero tener conto dello stato dell'arte, dei costi di attuazione, della natura dell'oggetto, del contesto e delle finalità del trattamento, e del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
Il regolamento impone di mettere in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire nel più breve tempo possibile se c'è stata una violazione dei dati personali, e se la gravità della violazione sia tale da rendere necessario l'obbligo di notifica. Infatti il GDPR introduce l'obbligo di notificare una violazione dei dati personali all'autorità Garante della protezione dei dati personali e, in alcuni casi, di comunicare la violazione alle singole persone fisiche i cui dati personali sono stati interessati dalla violazione.

Ruoli e responsabilità

Chiunque accerti o ipotizzi una violazione dei dati personali (vedi paragrafo "Cos'è la violazione dei dati personali (Data Breach)") deve immediatamente avvisare il DPO aziendale (vedi "La notifica al DPO").
Il responsabile del trattamento impattato, coadiuvato dal DPO, effettua le valutazioni del caso e, in caso di rilevazione di un data breach, mette in atto tutte le attività volte ad arginare e comunicare l'evento, ovvero:

- Applicare ogni misura di sicurezza necessaria ad arginare il data breach (vedi "Arginare il data Breach")

- Effettuare una valutazione dell'impatto della violazione dei dati sulla sicurezza e sulle libertà degli interessati coinvolti (vedi "Arginare il data Breach")
- Compilare il registro delle violazioni (vedi "Il registro delle violazioni")
- Effettuare la notifica al Garante (vedi "La notifica al Garante")
- Effettuare la notifica agli interessati (vedi "La notifica all'Interessato")

Arginare il data Breach

A seguito di ricezione della segnalazione da parte di uno degli attori, il Titolare del trattamento, tramite il DPO, effettua la registrazione della segnalazione e, al fine di stabilire se si sia effettivamente verificato un Data Breach e se sia necessaria un'indagine più approfondita dell'accaduto, attiva una valutazione preliminare riguardante l'episodio stesso (fase di risk assessment).
Nel caso in cui si individuasse una possibile violazione di dati contenuti in un sistema informatico, il DPO, coadiuvato dall'Amministratore di Sistema, effettua un'istruttoria e le valutazioni di competenza in merito all'accaduto, attraverso l'esame delle seguenti informazioni:

- la data di scoperta della violazione (tempestività);
- Il soggetto che ha rilevato la violazione
- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- le eventuali azioni già intraprese.

A termine della fase di valutazione preliminare, nel caso si sia rilevata una possibile violazione dei dati, il Titolare del trattamento per il tramite del Responsabile della Protezione dei Dati e, in caso di violazioni informatiche, dell'Amministratore di sistema, mette in atto le azioni opportune al fine di stabilire:

- le misure correttive e di protezione che possano limitare i danni che la violazione potrebbe causare o aver causato (ad esempio, riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso… ecc.);
- le modalità e le tempistiche delle misure correttive, individuando gli attori e i compiti per la risoluzione della violazione;
- la necessità di comunicare la violazione all'Autorità Garante per la Protezione dei dati personali;
- la necessità di comunicare la violazione agli interessati.

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Responsabile delle Protezione dei dati valuterà la gravità della violazione utilizzando un modello standardizzato, secondo le indicazioni di cui all'art. 33 GDPR.

La valutazione del rischio

Previa valutazione del rischio, il data breach può essere comunicato al Garante. Il considerando 85 del GDPR spiega che lo scopo della notifica è di limitare i danni che possono derivare per effetto di una violazione a carico degli interessati e che l'efficacia di questo dovere di limitazione dipende dalla tempestività e dall'adeguatezza con cui la violazione è affrontata.
Il gruppo "Article 29 Data Protection Working Party" (WP 29), chiarisce ulteriormente che la responsabilità del titolare deve essere commisurata secondo la sua capacità di scoprire tempestivamente un incidente ed indagarlo al fine di valutare l'obbligatorietà della notifica.
In definitiva il nucleo centrale su cui è necessario lavorare nella fase investigativa è quella di capire in tempi brevi, l'impatto che il potenziale attacco ha avuto sui dati personali delle varie categorie di interessati. Occorre valutare preliminarmente non solo "come" è avvento l'attacco, ma "cosa" sia stato oggetto di attacco.
Si possono distinguere tre tipi di violazione:

1. **Confidentiality Breach** (violazione della riservatezza), in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;

2. **Integrity Breach** (violazione dell'integrità), in caso di modifica non autorizzata o accidentale dei dati personali;

3. **Availability Breach** (violazione della disponibilità), in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Una violazione può riguardare ovviamente anche più di una tipologia allo stesso momento. Mentre stabilire se vi sia stata una violazione della riservatezza o dell'integrità è relativamente evidente, può essere meno ovvio determinare se vi è stata una violazione della disponibilità. Una violazione sarà sempre considerata una violazione della disponibilità se si è verificata una perdita o una distruzione permanente dei dati personali.
Ci sono alcuni fattori da tenere in considerazione per determinare la gravità del rischio:

i. il tipo di violazione: è evidente che il tipo di violazione determina un parametro per la valutazione del rischio.
ii. la natura, il numero e il grado di sensibilità dei dati personali violati
iii. la facilità di associare i dati violati ad una persona fisica
iv. la gravità delle conseguenze per gli interessati
v. il numero di esposti al rischio
vi. le caratteristiche del titolare del trattamento

Dato che l'obbligo di notifica spetta al titolare, è molto importante che questi, nell'affidare servizi a responsabili del trattamento, preliminarmente ci si accerti delle loro capacità di gestire tempestivamente e adeguatamente un incidente di sicurezza (art. 28 p.1 GDPR) e, quindi, preveda idonee clausole contrattuali (art. 28 p.3 GDPR) che regolino il rapporto di fornitura in modo da garantire il rispetto del GDPR.
L'art. 33 p.2 GDPR prevede espressamente il dovere del responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.
Scoprire l'incidente non è sufficiente, il titolare deve essere in grado di valutare la portata di questo in termini di impatto rispetto ai dati personali ed ai diritti e le libertà degli interessati.
Anche un incidente che determini la non disponibilità di dati per un periodo di tempo deve essere comunque considerato violazione e deve essere comunque documentato, in quanto la mancanza di accesso ai dati può avere
un impatto significativo sui diritti e sulle libertà delle persone fisiche.
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 (vedi paragrafi successivi). 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. A norma dell'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.
Occorre valutare la possibilità che la violazione possa causare danni fisici, materiali o immateriali alla persona fisica. Il considerando 85 GDPR a titolo d'esempio elenca alcuni casi: perdita del controllo dei dati personali che li riguardano; limitazione dei loro diritti; discriminazione; furto o usurpazione di 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 per la persona interessata.
L'art. 34 del GDPR stabilisce che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e la libertà delle persone fisiche, il titolare deve comunicare la violazione all'interessato senza ingiustificato ritardo.
Il considerando 86 del GDPR chiarisce che l'obbligo di comunicazione risponde allo scopo di consentire all'interessato, qualora sussista una violazione che presenti rischi elevati, di prendere le precauzioni necessarie.
La comunicazione ha un contenuto pressoché identico a quello della notifica.

Il registro delle violazioni

La ASL Taranto tiene un registro delle violazioni costantemente aggiornato man mano che eventuali episodi di data breach si verificano.
Il registro delle violazioni è un file excel in cui devono essere riportate le seguenti informazioni per ogni evento di data breach:

- Evento: denominazione dell'evento
- descrizione dettagliata dell'evento: Descrizione con un linguaggio semplice e chiaro della natura della violazione dei dati personali
- data e ora dell'accadimento
- segnalante: persona che ha emesso la segnalazione
- luogo della violazione: ufficio o struttura o reparto o sistema informatico o altro luogo in cui si è verificata la violazione
- modalità della violazione: in che modo si è verificata la violazione
- tipologia della violazione: confidentiality / Integrity / availability breach
- sistemi impattati: sistemi informativi impattati dallaviolazione
- tipologia di dati impattati: dati personali identificativi, sensibili, ultra sensibili…
- tipologia degli interessati: cittadini, assistiti, medici di base, personale, etc
- numero di Interessati: indicare approssimativamente o per classi il numero di interessati vittime della violazione
- notifica agli interessati (si/no): indicare se è necessaria o se è stata fatta la notifica agli interessati
- modalità della notifica/ motivazione notifica non avvenuta: se è necessaria la notifica agli interessati, indicare in che modo essa debba/è stata fatta (via mail, telefono, lettera, media locali, regionali, nazionali…)
- conseguenze della violazione: 1 perdita di dati; 2 rischio per i diritti e le libertà degli interessati; 3 violazione della integrità dei dati;
- motivazioni supplementari sulle conseguenze: indicare ad esempio, se il dato è criptato, se c'è stato furto di dati, indicare che la criptazione rende inutilizzabile il dato sottratto, etc
- tempo di ripristino del servizio: indicare il tempo necessario a ripristinare il servizio nelle sue funzionalità complete
- azioni effettuate / piano d'azione per il ripristino: indicare che cosa è stato fatto / cosa si prevede di fare per ripristinare il sistema in sicurezza
- data/ora comunicazione al Garante (se applicabile): indicare quando è stata fatta la comunicazione al Garante, qualora la valutazione del rischio lo abbia reso necessario
- motivazione mancata notifica al Garante : indicare quali sono state le motivazioni a supporto della mancata notifica.
- data di chiusura: quando tutta l'operazione di intervento sul data breach è stata conclusa
- misura/e di sicurezza violata/e: ad esempio aggiramento del firewall di rete, apertura armadio, apertura stanza, etc.
- impatto del ripristino sulla/e misura/e di sicurezza violata/e: indicare se il ripristino delle misure di sicurezza violate abbiano risolto il problema o se sussiste un allarme per i dati presenti e/o violati
- valutazione gravità della violazione: indicare la gravità della violazione (bassa, media, alta)
- note: eventuali altre informazioni che si ritenga utile evidenziare

Il monitoraggio degli eventi di potenziale violazione

La rilevazione degli eventi di data breach avviene oltre che per segnalazione diretta, anche mediante la segnalazione da parte di strumenti automatici di rilevazione di eventi di violazione dei dati.
Il monitoraggio viene effettuato tramite il controllo delle attività di trattamento definite nel Registro dei trattamenti, in particolare per quei trattamenti che sono stati valutati con rischio medio o elevato in fase di Valutazione d'Impatto.

Le attività di monitoraggio possono avvenire tramite gli opportuni sistemi di sicurezza ICT gestiti dall'amministratore di sistema e dagli incaricati dei CED, per tutti gli eventi che possono accadere via rete o che impattano sui prodotti software o hardware, ma è necessario anche monitorare i luoghi fisici in cui i dati personali vengono trattati, mantenuti o archiviati, con particolare riferimento ai dati sensibili. Il DPO è la figura preposta a tali controlli, con il supporto dei responsabili e degli incaricati di volta in volta coinvolti per competenza.

La notifica al DPO

Chiunque accerti o sospetti un episodio di violazione dei dati, deve immediatamente comunicare l'evento al DPO tramite segnalazione via mail all'indirizzo dpo@asl.taranto.it o dpo.asl.taranto@pec.rupar.puglia.it.
La comunicazione dovrà contenere:

- Identificativo del segnalante
- ufficio /struttura /reparto in cui l'evento si è verificato
- il tipo di violazione
- data presunta in cui la violazione è avvenuta
- eventuali conseguenze ipotizzabili dalla violazione
- un livello approssimativo autovalutato di gravità (bassa, media, alta)
- i dati di contatto del segnalante affinché possa essere contattato dal DPO

La notifica al Garante

L'art.33 GDPR impone al titolare del trattamento la notifica all'autorità di controllo competente di una eventuale violazione dei dati personali (data breach) senza ingiustificato ritardo, ovvero entro 72 ore dal momento in cui ne è venuto a conoscenza.
Se la notifica avviene dopo le 72 ore, deve essere corredata da elementi giustificativi.
L'obbligo non sussiste se *è improbabile* che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
L'obbligo di notifica al garante ha anche il fine di consentire all'autorità di controllo di verificare il rispetto della norma.
Ne discende che le generali attività di scoperta dell'incidente, come le successive di trattamento, devono essere documentate, adeguate, (devono riportare le violazioni, le circostanze, le conseguenze ed i rimedi), tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti.
È importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.
Il tempo di decorrenza dalla scoperta del data breach decorre dal momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali. Dunque il titolare del trattamento è tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate.
Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipende dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. In ogni caso l'accento viene posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario. Nel tempo necessario per indagare se si è effettivamente verificato un eventuale evento di violazione dei dati, non si ritiene che il Titolare sia a conoscenza del data breach, in quanto è in corso appunto una attività di accertamento che deve comunque essere svolta prima e nel più breve tempo possibile.
La notifica al garante deve essere effettuata via mail all'indirizzo

databreach.pa@pec.gpdp.it.

La notifica all'Interessato

La comunicazione della violazione alle persone fisiche interessate consente al titolare del trattamento di fornire loro informazioni sui rischi derivanti dalla violazione e sui provvedimenti che esse possono prendere per proteggersi dalle potenziali conseguenze della violazione. Qualsiasi piano di risposta alle violazioni dovrebbe sempre mirare a proteggere le persone fisiche e i loro dati personali.
Ai sensi dell'art.34, se la violazione dei dati è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, la notifica va rivolta anche all'interessato, senza ingiustificato ritardo.
La comunicazione del Data Breach all'interessato deve essere effettuata utilizzando un linguaggio semplice e chiaro e deve riportare la natura della violazione, le possibili conseguenze e le misure adottate o di cui si prevede l'adozione da parte del titolare, per attenuarne i possibili effetti negativi.
All'interessato vanno comunicate, con uno dei mezzi disponibili, le seguenti informazioni:

- Dati di contatto del DPO a cui potersi riferire per ogni eventualità in merito;
- Una descrizione dell'evento occorso e dell'impatto probabile sui propri dati personali;
- Le misure adottate o che si intendono adottare per risolvere il problema e/o attenuarne il possibile impatto sull'interessato.

La notifica all'interessato non è dovuta se:

- Il titolare del trattamento ha messo in atto le misure tecniche e organizzative di protezione adeguate, ovvero che rendano il dato non intellegibile a chiunque non sia autorizzato ad accedervi (cifratura, pseudonimizzazione, etc.);
- Il titolare del trattamento ha successivamente adottato le misure atte a scongiurare i rischi per i diritti e le libertà degli interessati;
- Tale comunicazione richiederebbe sforzi sproporzionati (ad esempio il rischio include un numero molto elevato di interessati). In questo caso si procede ad una comunicazione pubblica o ad una misura simile tramite la quale gli interessati vengono informati con analoga efficacia.

La comunicazione della violazione dei dati deve essere distinguibile rispetto ad ogni altra comunicazione fatta agli interessati e deve richiamare l'attenzione degli stessi.
È opportuno quindi dotarsi preventivamente di un opportuno piano di comunicazione, considerando la qualità dei dati sensibili trattati dalla ASL Taranto e il rischio elevato per i diritti e le libertà degli interessati in caso di violazione dei dati.
La comunicazione è soddisfatta allorquando:

- Il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure (in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura) erano già state applicate ai dati personali prima della violazione;
- Il titolare del trattamento, in seguito alla violazione subita, ha adottato le misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.

Mentre per far scattare l'obbligo di notifica al Garante è sufficiente che sussista una violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche, per la comunicazione agli interessati occorre che tale rischio sia elevato.
Quest'ultima affermazione, oggetto del GDPR, comporta che il titolare debba essere in grado di valutare il livello di rischio di qualsiasi tipo di violazione di dati personali trattati.
In caso di dubbio se sia necessario o meno effettuare la comunicazione verso gli interessati, all'atto della notifica all'autorità di controllo, il titolare del trattamento può ottenere consulenza sull'eventuale necessità di informare le persone fisiche interessate. In ogni caso l'autorità di controllo può ordinare al titolare del trattamento di informare le persone fisiche interessate dalla violazione.

Sanzioni

L'eventuale ritardo nella notifica deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nelle condizioni di applicare le misure correttive a sua disposizione ovvero:

l'esercizio dei poteri previsti dall'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposte di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), l'imposizione di sanzioni amministrative secondo l'art. 83 GDPR, il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.
Occorre in ogni caso tenere conto che, la mancata notifica e/o comunicazione, possono rappresentare per l'autorità di controllo un indizio di carenze più profonde e strutturali quali ad esempio carenza od inadeguatezza di misure di sicurezza, in tal caso, trattandosi di ipotesi separate ed autonome, l'autorità procederà per l'ulteriore irrogazione di sanzioni.
Il rispetto degli obblighi di notifica (art. 33) e di comunicazione (art. 34), in situazioni già mediamente complesse (in termini di dimensioni ed articolazione dell'organizzazione del titolare e/o in termine di numero di interessati di cui sono trattati i dati personali e/o in termini di operazione del trattamento, o di quantità, varietà, natura dei dati trattati), richiede al Titolare di strutturare il trattamento dei dati personali avvalendosi di un sistema di conformità e gestione del rischio che preveda un sotto-sistema per la gestione degli incidenti e la continuità operativa.
Questo sistema deve essere in grado di rispettare i requisiti di trasparenza, evidenza e responsabilità prescritti dal GDPR; si ricorda che l'art. 24 punto 1 del GDPR richiede al titolare di "mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR ".