Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016

Procedura di risposta ad una violazione dei dati personali

1. Generalità

Il Regolamento UE 2016/679 stabilisce che si manifesta una violazione dei dati personali (*data breach*) quando avviene una violazione di sicurezza che determina, 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 dal Responsabile per conto del Titolare, che comporti un rischio per per i diritti e le libertà delle persone fisiche.

Rientrano nella fattispecie gli eventi e i comportamenti atti a danneggiare i dati, a comprometterne la disponibilità o l'integrità indipendentemente da finalità o interventi fraudolenti, nonché gli incidenti avvenuti per fatti accidentali che compromettono l'integrità dei dati.

Fatti simili si verificano nella gestione e conservazione di dati con supporti informatici e tecnologici, ma assumono rilevanza per l'art. 33 del Regolamento UE 2016/679 quando la violazione dei dati personali presenta un rischio per i diritti e le libertà delle persone fisiche.

La corretta gestione del *data breach* ed in particolare la valutazione degli aspetti di rilevanza giuridica, organizzativa, tecnica e tecnologica, nonché quelli inerenti gli interventi posti in essere hanno una notevole rilevanza per limitare le conseguenze sui diritti e le libertà personali degli interessati e per prevenire o evitare eventuali conseguenze di carattere economico-finanziarie dovute a pretese risarcitorie e danni per l'Amministrazione regionale.

2. La violazione di sicurezza

Il Gruppo di lavoro articolo 29, istituito dall'Unione Europea, ha individuato nelle sue linee guida del 6/2/2018 in materia di *data breach*, tre categorie di eventi rilevanti ai sensi degli artt. 33 e 34 del Regolamento:

- quando vi è un accesso incidentale o abusivo a dati personali;
- quando vi è una perdita o distruzione accidentale o non autorizzata del dato personale;
- quando vi è un'alterazione accidentale o non autorizzata del dato personale.

Nel caso concreto la violazione può riguardare anche più di una di queste categorie.

Per valutare la presenza di un rischio per i diritti e le libertà delle persone fisiche evidenzia, vanno considerati i seguenti elementi:

- il tipo di violazione;
- la natura, il numero e il grado di sensibilità dei dati personali violati;
- la facilità di associare i dati violati a una persona fisica;
- la gravità delle conseguenze per gli interessati;
- il numero di interessati esposti al rischio;
- le caratteristiche del titolare del trattamento come, per esempio, le dimensioni dell'ente, il tipo di attività svolta, la qualità e quantità di dati trattati.

3. La notifica al Garante della protezione dei dati personali

Il Regolamento stabilisce che il Titolare effettua le comunicazioni al Garante della protezione dei dati personali (Garante) sulla violazione di dati personali (art. 33) ed informa l'interessato se si presenta il rischio per i diritti e le liberta di quest'ultimo (art. 34).

Lo stesso articolo prevede che la notifica non sia necessaria laddove sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

4. Il Modello di notifica

Il modello che viene utilizzato è quello messo a disposizione dal Garante, disponibile anche nel sito della Regione Siciliana nella sezione del RPD.

Il modello da trasmettere al Garante:

- descrive la natura della violazione dei dati personali
- descrive le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunica il nome e i dati di contatto del Responsabile della protezione dei dati e di altro punto di contatto presso cui ottenere più informazioni;
- descrive le probabili conseguenze della violazione dei dati personali;
- descrive le 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.

5. La compilazione del Modello

Il modello va compilato dal Responsabile del trattamento con il supporto del sub-Responsabile e del Referente Privacy e avendo consultato il sub-Responsabile tecnico che cura la gestione informatizzata dei dati e viene quindi inviato al Titolare perché lo faccia proprio e provveda all'inoltro al Garante entro 72 ore dal momento in cui la violazione è conosciuta. Entro questo termine il Titolare deve essere in grado di identificare la violazione, revisionare eventuale documentazione, adottare procedure e/o atti che mitighino il danno arrecato e notificare il *data breach* al Garante.

6. La comunicazione all'interessato

L'art. 34 del Regolamento stabilisce che quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento debba comunicare la violazione all'interessato senza ingiustificato ritardo. Ciò al fine di consentire all'interessato di proteggersi da eventuali conseguenze dannose derivanti dal *data breach*.

La comunicazione all'interessato deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le informazioni e le misure di cui all'art. 33, paragrafo 3, lettere b), c) e d).

Il Titolare è esonerato dal comunicare il *data breach* all'interessato nel caso in cui:

- siano state implementate misure di sicurezza adeguate e tali misure erano già state applicate ai dati personali oggetto del *data breach* (per esempio la cifratura);
- dopo il *data breach* sono state adottate misure di sicurezza atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione all'interessato richiederebbe sforzi sproporzionati e quindi si può procedere a una comunicazione pubblica.

7. Il Registro delle Violazioni

Inoltre il Titolare documenta qualsiasi violazione dei dati personali, comprese le circostanze in cui è avvenuto, le conseguenze ed i provvedimenti adottati per porvi rimedio (art.33); per tali fini ciascun Titolare tiene un registro delle violazioni dei dati, che include le violazioni avvenute presso i Responsabili, i sub-Responsabili e i sub-Responsabili tecnici coinvolti nei trattamenti di dati personali di ciascun Titolare.

Il Registro potrà essere esaminato dal Garante per verificare il rispetto delle norme in materia.

Il Registro deve riportare:

- le circostanze relative a qualsiasi violazione dei dati personali e le sue conseguenze;
- i provvedimenti adottati per porvi rimedio.

Inoltre il Titolare deve motivare le decisioni assunte, riportandole nel Registro, in particolare nel caso in cui abbia deciso di non procedere alla notifica, oppure abbia ritardato nella procedura di notifica, oppure abbia deciso di non comunicare il *data breach* agli interessati.

Al fine di catalogare unitariamente le violazioni il RPD coordina la realizzazione e il funzionamento di un sistema informativo per l'intera Amministrazione regionale per la tenuta dell'elenco delle Violazioni di dati che sarà utilizzato dai Titolari e dai Responsabili e ne sorveglia l'aggiornamento.
La documentazione delle violazioni avvenute consente al Titolare, assistito dal Responsabile, di aggiornare regolarmente i processi per adottare tutte le misure tecniche e organizzative più appropriate, alla luce delle criticità evidenziate dagli eventi accaduti.

8. La procedura in caso di *data breach*

La procedura di *data breach* si articola nelle seguenti fasi:

a) comunicazione del fatto: il soggetto che venga a conoscenza di un fatto o di una circostanza che determini o possa determinare una violazione dei dati personali informa, senza ingiustificato ritardo, il Titolare del trattamento, il Responsabile del trattamento, il sub-Responsabile, il sub-Responsabile tecnico, il Referente Privacy e il RPD inviando una segnalazione per posta elettronica o telefonica. Qualora la segnalazione sia effettuata da un interessato e pervenga ad un solo dei soggetti sopra elencati, questi provvede ad informarne gli altri;
b) accertamento della violazione: il Referente Privacy, supportato dal sub-Responsabile e, nel caso di dati informatizzati, dal sub-Responsabile tecnico, acquisisce le informazioni sulla segnalazione, sul contesto, sugli effetti della violazione e ogni ulteriore informazione utile all'accertamento della violazione;
c) valutazione della violazione: il Referente Privacy, supportato dal sub-Responsabile e, nel caso di dati informatizzati, dal Sub-Responsabile tecnico effettua un prima valutazione sul fatto descritto in base degli elementi acquisiti, sul rischio per i diritti e le libertà delle persone fisiche interessate. Qualora si possa considerare ragionevolmente certo che il rischio per i diritti e le libertà delle persone fisiche non sia elevato, comunica in forma scritta al Responsabile, al Titolare e al RPD la valutazione e procede alla semplice registrazione dell'evento nel Registro delle violazioni.
d) comunicazione al Garante: qualora non possa considerarsi ragionevolmente certo un rischio significativo per i diritti e le libertà dell'interessato, il Referente Privacy supportato dal sub-Responsabile e, nel caso di dati informatizzati dal sub-Responsabile tecnico, predispone il modello di notifica della violazione al Garante, lo consegna al Responsabile per la sua trasmissione al Titolare, affinché quest'ultimo possa procedere alla notifica senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. Se non è rispettato il termine delle 72 ore, il ritardo dev'essere giustificato adducendo una adeguata motivazione. La notifica è effettuata con nota protocollata, inviata tramite PEC. Copia del modello e degli altri atti connessi viene conservato agli atti ed anche inviato al RPD;
e) comunicazione all'interessato: il Titolare, assistito dal Responsabile e con il supporto del Referente Privacy, del sub-Responsabile e del Sub-Responsabile tecnico, comunica la violazione all'interessato senza ingiustificato ritardo e in maniera chiara e trasparente, tramite l'invio di una mail o, in mancanza, altra forma di comunicazione (per es. telefonica o cartacea). Nel caso in cui ci siano più interessati e la comunicazione diretta richiederebbe sforzi ingenti si procede a una comunicazione pubblica, o misura simile, tramite la quale gli interessati sono informati con analoga efficacia, per es. pubblicazione di un avviso evidente nella home page del portale istituzionale per un congruo numero di giorni oppure notifica sempre tramite il portale istituzionale (art. 34).
f) il Responsabile con il supporto del Referente Privacy, del sub-Responsabile e, ove presente il sub-Responsabile tecnico, dispone quanto necessario affinché si provveda con urgenza ai

primi adempimenti per limitare le conseguenze dell'evento e per evitare il ripetersi a breve termine dell'evento. Di ciò informa il RPD;

g) compilazione del registro: il Titolare del trattamento, assistito dal Responsabile e con il supporto del Referente Privacy documenta i fatti nel registro delle violazioni, ed in particolare le circostanze relative a qualsiasi violazione dei dati personali le sue conseguenze, i provvedimenti adottati per porvi rimedio e la motivazione delle decisioni assunte, in particolare nel caso in cui abbia deciso di non procedere alla notifica, ed eventuali ritardi con le rispettive cause.
h) il Titolare, assistito dal Responsabile, con il supporto del Referente Privacy, del sub-Responsabile e del Sub-Responsabile tecnico effettua una valutazione di opportunità sul procedere ad una approfondita Valutazione di impatto sui dati personali sul trattamento interessato dalla violazione e in merito consulta il RPD;
i) il Titolare, assistito dal Responsabile, con il supporto del Referente Privacy, del sub-Responsabile e del sub-Responsabile tecnico mette in atto tutti i provvedimenti definitivi ritenuti necessari anche sulla scorta degli esiti dell'eventuale Valutazione di impatto condotta. Di ciò informa il RPD.

Esempi di Violazioni di sicurezza

Si riportano nel seguito alcuni esempi di violazioni di sicurezza:

- un attacco informatico ad uno o più sistemi informativi
- la distruzione o perdita di dati per cause differenti da un attacco informatico o da problemi tecnici;
- un'interruzione del servizio di un sistema di gestione dati dell'Amministrazione causato ad esempio da una interruzione di energia elettrica, che rende i dati personali non più disponibili;
- la impossibilità di accedere a dati crittografati qualora sia andata persa la chiave di decrittografia;
- il furto o smarrimento di un computer portatile, di un cellulare di servizio non opportunamente cifrato;
- lo smarrimento di una chiavetta USB che contiene dati personali di dipendenti o cittadini.