La violazione dei dati personali (data breach)

4 Dicembre 2018

1. Premessa

Il Regolamento UE 2016/679 relativo alla protezione delle persona fisiche con riguardo al trattamento dei dati personali (di seguito anche Regolamento) prevede che i dati personali possano essere trattati soltanto a seguito dell'adozione di misure tecniche ed organizzative adeguate ad assicurare loro un appropriato livello di sicurezza dai rischi.

Elemento rilevante nella politica di sicurezza è di essere in grado, ove possibile, di prevenire incidenti e violazioni di dati e di reagire in modo tempestivo nel caso in cui comunque accadano.

2. Che cos'è una violazione di dati personali?

Il Regolamento definisce violazione dei dati personali 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, punto 12)

> *Esempio:*
>
> *Si ha perdita di dati personali quando viene perso o rubato un dispositivo che contiene la copia di un data base con dati personali, o quando l'unica copia di un set di dati personali è stata criptata da un ransomware oppure quando i dati sono stati criptati dal Titolare usando una chiave di cui ha perso il possesso.*

3. Tipi di violazioni

Il Gruppo di lavoro europeo sulla protezione dei dati personali – Working Party art. 29 o WP29 - ha individuato tre categorie di violazioni:

- *violazione della confidenzialità del dato*: nel caso in cui vi sia una divulgazione o un accesso ai dati personali, accidentale o non autorizzata;

- *violazione dell'integrità del dato*: in caso di alterazione accidentale o non autorizzata di dati personali;
- *violazione della disponibilità del dato*: nel caso di perdita di accesso o distruzione di dati, accidentale o non autorizzata.

A seconda delle circostanze, una violazione può riguardare singolarmente o contemporaneamente la confidenzialità, l'integrità o la disponibilità di dati o combinazioni di esse.

> *Esempio*
>
> *Si ha una perdita di disponibilità del dato quando il dato è stato cancellato (accidentalmente o da persona non autorizzata), oppure, nel caso di dati protetti mediante criptazione, quando è andata perduta la chiave di decriptazione.*
>
> *Perdita di disponibilità può verificarsi inoltre a seguito di un attacco di denial of service che rende il dato personale non disponibile.*

4. Gli adempimenti in caso di violazione dei dati personali.

4.1 La notificazione al Garante

Il Regolamento dispone all'art. 33 che le violazioni dei dati personali debbano essere notificate dal Titolare del trattamento al Garante entro 72 ore dal momento in cui ne sia venuto a conoscenza, a meno che risulti improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. In attuazione di quanto disposto dalla deliberazione del Consiglio Direttivo INFN n. 14844 del 27 luglio 2018, il compito di provvedere alla notifica della violazione è attribuito ai Direttori delle Strutture, nonché ai Direttori delle articolazioni dell'Amministrazione Centrale ed ai Responsabili del Servizio di Presidenza e dell'Ufficio Comunicazione dell'INFN

Il fine della notificazione è quello di sollecitare una pronta reazione in caso di violazione di dati, per contenerla, recuperare i dati compromessi ed ottenere indicazioni rilevanti dall'Autorità Garante. La notificazione al Garante nelle 72 ore consente di assicurare che, in base alle caratteristiche della violazione rilevata, la decisione di notificare o meno la violazione anche ai soggetti interessati sia corretta.

Anche un incidente di sicurezza che renda non disponibili i dati personali solo temporaneamente può costituire una violazione che deve essere notificata, tuttavia occorre accertare le circostanze della violazione e capire se è necessario effettuare la notifica al Garante ed anche la comunicazione agli interessati.

> *Esempio*
>
> *In un contesto ospedaliero se dati medici dei pazienti sono resi indisponibili anche temporaneamente, può ravvisarsi un rischio ai diritti e alle libertà delle persone, perché ad esempio possono essere cancellati interventi operatori, mettendo a rischio la vita delle persone.*
>
> *In un diverso contesto: se i sistemi di una ditta di comunicazione diventano inutilizzabili per alcune ore (per esempio per un'interruzione di corrente) e la ditta non ha potuto inviare la newsletter agli iscritti, difficilmente si potrà parlare di rischio ai diritti e alle libertà delle persone.*

Sebbene una perdita di disponibilità dei sistemi possa essere solo temporanea e non avere impatto sulle persone, è importante considerare tutte le conseguenze della violazione che possono richiedere la notificazione per altre ragioni. La violazione di dati può determinare significativi effetti sfavorevoli per le persone e cagionare danni fisici, materiali o immateriali quali limitazione di diritti, discriminazioni, furti d'identità, frode, perdite finanziarie, danni alla reputazione e così via. È importante quindi individuare le violazioni per poter tempestivamente effettuare la notificazione se dovuta.

> *Esempio*
>
> *Un'infezione da ransomware può portare ad una perdita temporanea di disponibilità se i dati possono essere recuperati da un backup, tuttavia c'è stata un'intrusione e la notificazione potrebbe essere dovuta se l'incidente si qualifica come perdita di confidenzialità che comporti un rischio per i diritti e le libertà delle persone.*

4.1.1 Quando si ha conoscenza della violazione?

Come detto, i soggetti individuati nella deliberazione C.D. n. 14844/2018 devono notificare la violazione al Garante senza ingiustificato ritardo e, se possibile, entro 72 ore da quando ne hanno avuto conoscenza. Quando si possa dire di avere conoscenza di una violazione dipende dal caso concreto.

> *Esempi*
>
> *Nel caso di perdita di una chiavetta USB con dati personali non criptati spesso non è possibile verificare quando persone non autorizzate abbiano avuto accesso ai dati, tuttavia, anche se non si può stabilire se c'è stata violazione di confidenzialità, il caso deve essere notificato perché c'è una ragionevole certezza che una violazione di disponibilità sia accaduta.Il Titolare ne ha conoscenza quando ha saputo che la chiavetta USB è stata persa.*
>
> *Un soggetto terzo informa il Titolare di aver ricevuto i dati personali di uno dei suoi clienti e dà evidenza di una divulgazione non autorizzata. Nel momento in cui al Titolare è stata data chiara evidenza di una violazione di confidenzialità, egli ne è a conoscenza.*
>
> *Un Titolare rileva che può esserci stata un'intrusione nella sua rete. Egli verifica i sistemi per stabilire se i dati personali in essi contenuti sono stati compromessi e ne trae conferma. Ancora una volta il Titolare ha chiara evidenza della violazione e non può esserci dubbio che ne sia a conoscenza.*
>
> *Un cyber criminale contatta il Titolare, dopo aver attaccato i suoi sistemi, per chiedere un riscatto. Se la verifica dei sistemi conferma che c'è stato un attacco, allora è a conoscenza della violazione.*

Dopo essere stato informato di una potenziale violazione il soggetto tenuto alla notifica può aver bisogno di un breve periodo di tempo per accertare se effettivamente la violazione ci sia stata. Durante questo periodo non si può ritenere che abbia conoscenza della violazione, tuttavia egli se ne deve accertare il più velocemente possibile e con un ragionevole grado di certezza.

Una volta accertata la violazione, deve provvedere alla notifica senza ingiustificato ritardo e ove possibile non oltre le 72 ore. Se effettua la notificazione successivamente a tale periodo, deve indicare i motivi del ritardo.

In caso di contitolarità, l'accordo che disciplina la contitolarità deve individuare, tra l'altro, anche quale contitolare abbia la responsabilità di provvedere all'obbligo di notifica.

Anche nel caso in cui i dati siano affidati ad un Responsabile (soggetto esterno) il contratto che disci-

plina i rapporti tra Titolare e Responsabile deve prevedere che il Responsabile dia notizia al Titolare di eventuali violazioni “senza ingiustificato ritardo”.

4.1.2. Informazioni da fornire al Garante in sede di notifica

Secondo quanto stabilito all’art. 33, comma 3, del Regolamento, nella notifica della violazione è necessario:

a. descrivere la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione (sebbene il Regolamento non definisca cosa intenda per categorie di soggetti interessati, il WP29, fornisce degli elementi per la classificazione, esemplificando alcune categorie, tra cui quelle composte da bambini, da gruppi vulnerabili, come le persone con disabilità, il personale dipendente, o i consumatori);
b. comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c. descrivere le probabili conseguenze della violazione dei dati personali;
d. descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

La mancanza di informazioni precise circa la violazione rilevata non costituisce ostacolo per una notificazione tempestiva: in questi casi il Regolamento richiede una prima notificazione per approssimazione circa il numero di persone coinvolte, le categorie di interessati e tipologie di dati violati, consentendo di fornire ulteriori dettagli in seguito, con una notificazione per fasi. Si fornisce in allegato un modello da utilizzare per la notifica al Garante.

4.1.3 La notificazione per fasi

A seconda della natura della violazione, possono rendersi necessarie ulteriori indagini per individuare tutti gli aspetti rilevanti di una violazione.

Il Regolamento all’art. 33, comma 4, dispone che “Qualora e nella misura in cui non sia possibile fornire informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ritardo”.

Nel caso in cui ci siano violazioni per incidenti di sicurezza complessi, nelle 72 ore successive al momento in cui è stata acquisita conoscenza della violazione è necessario procedere alla notificazione al Garante con i dati disponibili e procedere quindi alle ulteriori indagini per acquisire altri dettagli, da notificare successivamente e comunque senza ingiustificato ritardo.

In caso di notifica per fasi, è necessario informare il Garante che le informazioni trasmesse non sono complete e che ci saranno fasi successive di notificazione.

E’ necessario, inoltre, aggiornare il Garante anche se dalle indagini successive emerge che l’incidente non ha prodotto alcuna violazione di dati. Il WP29 chiarisce che non ci sono sanzioni per aver segnalato un incidente che in seguito si è rilevato non aver determinato violazioni.

> *Esempio*
>
> *Un Titolare notifica al Garante di aver rilevato una violazione per aver perso una chiavetta USB contenente copia di dati personali. La chiavetta in seguito viene ritrovata mal riposta, ma entro i locali del Titolare e recuperata. In questo caso il Titolare aggiorna il Garante e chiede che la precedente notificazione sia corretta.*

4.1.4 Notificazione tardiva

È consentita la notificazione di una violazione al Garante oltre le 72 ore ma in questo caso è necessario indicare le ragioni del ritardo.

Il WP29 ipotizza il caso di un Titolare che rileva una violazione e che durante l'indagine, prima della notifica, scopre ulteriori violazioni simili che hanno però cause diverse. A seconda delle circostanze, il Titolare può aver bisogno di tempo per stabilire le cause della violazione e decidere di predisporre una notificazione unica per tutte le violazioni con le diverse possibili cause.

4.2 La comunicazione ai soggetti interessati

Il Regolamento all'art. 34 dispone che "Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza giustificato ritardo".

È sempre dovuta la notificazione al Garante della violazione dei dati personali se dalla violazione possa derivare un rischio per i diritti e le libertà delle persone; quando tale rischio sia qualificabile come elevato, la violazione deve essere comunicata anche agli interessati (cioè ai soggetti a cui i dati si riferiscono).

Il rischio elevato sussiste quando la violazione può arrecare danni fisici, materiali o immateriali per coloro i cui dati sono stati violati. Tra questi la discriminazione, il furto d'identità, la frode, le perdite finanziarie o il danno alla reputazione. A maggior ragione se la violazione coinvolge dati personali che rivelano la razza, l'origine etnica, l'opinione politica, religiosa o filosofica o includono dati genetici o dati sulla salute o l'orientamento sessuale o informazioni connesse alla commissione di reati e conseguenti sanzioni o misure di sicurezza.

4.2.1 Informazioni da fornire agli interessati nella comunicazione della violazione

La comunicazione agli interessati deve contenere:

- una descrizione della natura della violazione.
- il nome ed i dettagli di contatto del DPO o di altro punto di contatto,
- una descrizione delle probabili conseguenze della violazione,
- una descrizione delle misure adottate o che il Titolare propone di adottare per affrontare la violazione, includendo le misure per mitigare i possibili effetti negativi.

A titolo d'esempio, il Titolare, dopo aver notificato la violazione al Garante, ha ricevuto da questo indicazioni sulla gestione della violazione e la riduzione del suo impatto: egli potrebbe fornire indicazioni specifiche agli interessati affinché si proteggano dalle conseguenze negative della violazione come il reset delle password se le loro credenziali di accesso sono state compromesse.

4.2.2 Come contattare gli interessati

La violazione deve essere comunicata alle persone interessate in modo diretto, salvo che questo comporti uno sforzo sproporzionato, con messaggi dedicati alla sola comunicazione della violazione. La violazione non deve essere comunicata nell'ambito di newsletter o messaggi generici. Il WP29 suggerisce, la messaggistica diretta (email, SMS) oppure banner evidenti in un sito web, o notificazioni o comunicazioni postali e raccomanda ai Titolari di individuare mezzi che massimizzino la possibilità di comunicare l'informazione in modo accurato a tutti gli interessati coinvolti.

La scelta della modalità di comunicazione e del linguaggio deve avere come fine quello di consentire agli interessati di comprendere la natura della violazione e le azioni che possono adottare per tutelarsi. Si fornisce in allegato un modello da utilizzare per la comunicazione agli interessati.

4.2.3 Casi nei quali la comunicazione agli interessati non è dovuta.

Il terzo comma dell'art. 34 individua tre ipotesi nelle quali non è dovuta la comunicazione agli interessati ed in particolare:

1. quando sono state adottate, prima della violazione, misure tecniche ed organizzative adeguate per la protezione dei dati, in particolare quelle misure che rendono i dati non intellegibili ai soggetti non autorizzati (p.e. cifratura);
2. quando, immediatamente dopo la violazione, sono state adottate misure che scongiurino il concretizzarsi di un alto rischio per i diritti e le libertà delle persone (p.e. sono state immediatamente individuate ed adottate misure contro colui che ha avuto accesso ai dati, prima che abbia potuto fare qualsiasi cosa con i dati stessi): in questi casi bisogna tenere in considerazione la violazione di confidenzialità, valutando la situazione caso per caso;
3. quando contattare i singoli comporta uno sforzo sproporzionato: in questi casi è consentita una comunicazione pubblica o l'adozione di misure simili per contattare gli interessati in modo effettivo.

Occorre ricordare che, in conformità al principio di responsabilizzazione, è necessario dichiarare e dimostrare al Garante che si è verificata una o più delle ipotesi precedenti che fanno venir meno l'obbligo di notificazione.

5. La valutazione del rischio e del rischio elevato

Come detto il Regolamento introduce l'obbligo di notifica della violazione, tuttavia la notifica al Garante non deve essere effettuata se è improbabile che la violazione metta a rischio i diritti e le libertà degli individui;

mentre la comunicazione agli interessati deve essere effettuata soltanto se si evidenzi un alto rischio per i diritti e le libertà.

Questo significa che, immediatamente dopo aver avuto conoscenza di una violazione, è importante non solo cercare di contenere l'incidente, ma valutare il rischio che può derivarne. Questo per almeno due motivi:

- la conoscenza e la potenziale gravità dell'impatto sugli individui aiuterà ad adottare misure effettive per affrontare l'incidente;
- la valutazione aiuterà ad individuare se deve essere fatta la notificazione al Garante e se deve essere data, oppure no, comunicazione ai singoli.

5.1 Fattori da tenere in considerazione per la valutazione del rischio

I considerando 75 e 76 consigliano che nella valutazione del rischio si tenga in considerazione sia la probabilità sia la gravità del rischio per i diritti e le libertà delle persone. Il WP29 raccomanda che nella valutazione del rischio siano tenuti in considerazione i seguenti criteri:

- il tipo di violazione,
- la natura, sensibilità e volume dei dati personali,
- l'agevole identificazione degli interessati,
- la gravità delle conseguenze,
- le specifiche caratteristiche degli interessati,
- le specifiche caratteristiche dei Titolari,
- il numero di interessati coinvolti.

6 Responsabilità e registrazione delle violazioni

Il Regolamento dispone che si tenga un Registro nel quale documentare tutte le violazioni rilevate, i loro effetti e le misure adottate per porvi rimedio. Tale adempimento è legato al principio di responsabilizzazione ed alla necessità di consentire le verifiche al Garante. Il Regolamento non specifica per quanto tempo debba essere conservata questa documentazione: il periodo di conservazione, nel rispetto dei principi del trattamento dei dati personali e con la base giuridica che consente il trattamento è individuato in cinque anni.

Il WP 29 raccomanda che nel Registro siano documentate anche le decisioni adottate in caso di violazione, quali ad esempio il motivo per il quale si è ritenuto che la violazione non dovesse essere notificata al Garante o comunicata agli interessati o le ragioni per le quali si è ritenuto che la notificazione dovesse essere effettuata in ritardo