



Procedura di gestione delle “VIOLAZIONI DI DATI PERSONALI”

Fase	Responsabile	Data	Versione
Predisposizione	<i>Gruppo Privacy e RPD</i>	14.03.2018	Beta
Approvazione	<i>Deliberazione del Direttore Generale n. 533</i>	10.08.2018	1.0
Revisione	<i>Gruppo Privacy e RPD</i>	31.08.2021	2.0

Sommario

1. PREMESSA	1
2. DESTINATARI	4
3. INDIVIDUAZIONE POSSIBILI VIOLAZIONE DEI DATI IN AMBITO A.O. ORDINE MAURIZIANO	4
4. LE DIVERSE FASI	6
4.1. Scoperta e Qualificazione	6
4.2. Valutazione	6
4.3. Notifica (Art. 33 p.3)	7
4.3.1. Quando il titolare è ritenuto “a conoscenza” di una violazione?.....	8
4.3.2. Procedura di notifica.....	9
4.3.2.1. Self assessment.....	9
4.3.2.2. Autenticazione.....	10
4.3.2.3. Compilazione della notifica.....	10
4.3.2.4. Notifica integrativa.....	11
4.3.2.5. Annullare una notifica.....	12
4.3.2.6. Riscontri all’utente e al titolare.....	12
4.4. Comunicazione della violazione all’interessato (art. 34)	12

1. PREMESSA

I dati personali trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti (es. errori umani) o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.

Per “**Violazione di dati**” si 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).

La violazione di dati è un particolare tipo di incidente di sicurezza (non necessariamente soltanto informatica), per effetto del 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, in particolare quello di integrità e riservatezza.



Scopo della presente “Procedura” è quello di definire un quadro di riferimento unitario, da parte delle strutture amministrative e sanitarie dell’Azienda, dalla fase di “SCOPERTA” della violazione alla fase di “NOTIFICA”.

Il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative.

Il 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, dispone espressamente quanto segue:

Articolo 4 Definizioni

12) «**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

Articolo 33 Notifica di una violazione dei dati personali all’autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all’autorità di controllo competente a norma dell’articolo 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.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

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 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.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Tale documentazione consente all’autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34 Comunicazione di una violazione dei dati personali all’interessato

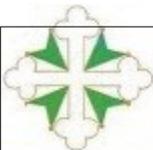
1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all’interessato senza ingiustificato ritardo.

2. La comunicazione all’interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all’articolo 33, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all’interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) 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;

b) 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;



c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta

L'art. 33 del **Regolamento Europeo 2016/679 (GDPR)** impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**), "ove possibile" entro settantadue ore dal momento in cui ne **viene a conoscenza**.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche; qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, "ove possibile" entro settantadue ore dal momento in cui il titolare ne viene a conoscenza; mentre l'eventuale comunicazione agli interessati, deve essere fatta senza ingiustificato ritardo.

L'eventuale ritardo nella notificazione deve essere, appunto, giustificato; il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR, il cui importo può arrivare a 10.000.000 di Euro (o, per le imprese, 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 carenze 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 all'autorità (art. 33) e di comunicazione della violazione all'interessato (art.34), in situazioni già mediamente complesse (in termini di dimensioni ed articolazione dell'organizzazione del titolare e/o in termini di numero di interessati di cui sono trattati i dati personali e/o in termini di operazioni di 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.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 p.5 del GDPR, prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma. Allo scopo l'Azienda adotta un **registro delle violazioni di dati (allegato C)**.



2. DESTINATARI

Destinatari della presente procedura sono tutti gli assegnatari di compiti e funzioni circa il trattamento di dati (designati e/o autorizzati), siano essi svolti con strumenti informatici o cartacei.

3. INDIVIDUAZIONE POSSIBILI VIOLAZIONE DEI DATI IN AMBITO A.O. ORDINE MAURIZIANO

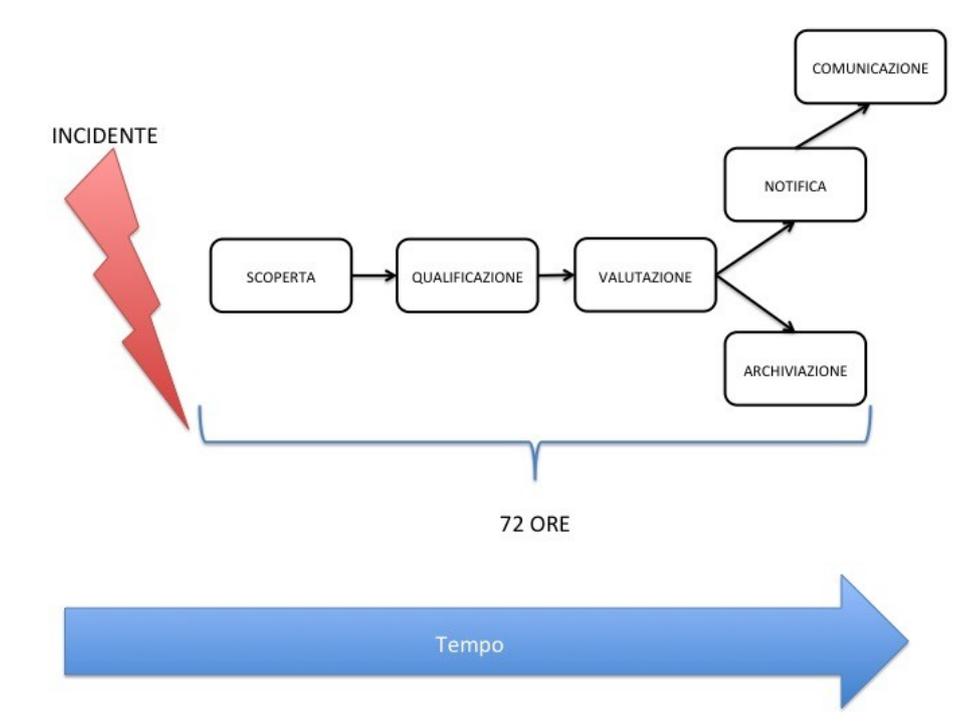
TRATTAMENTI INFORMATICI	COSA FARE	CHI DEVE FARLO (Funzionario Segnalante)	QUANDO DEVE FARLO	NOTIFICA
Furto Personal Computer e/o Portatile	Denuncia di furto e compilazione del modulo A allegato	Il dirigente della Struttura in cui è avvenuto il furto	Immediatamente, e in ogni caso entro 12 ore	Solo se nella dichiarazione (allegato A) emerge che sul PC rubato erano archiviati dati personali
Furto/perdita dispositivi mobili	Compilazione del modulo A allegato	Il titolare del dispositivo	Immediatamente, e in ogni caso entro 12 ore	Solo se nella dichiarazione (allegato A) emerge che sul dispositivo erano archiviati dati personali
Accesso non autorizzato ai dati e divulgazione degli stessi	Violazione di riservatezza. Messa in atto di misure idonee a contrastare tali eventi	Sistemi Informativi	Al momento della scoperta	Notifica se trattasi di dati personali
Modifica o alterazione dei dati	Violazione di integrità. Messa in atto di misure idonee a contrastare tali eventi	Sistemi Informativi	Al momento della scoperta	Notifica se trattasi di dati personali
Cancellazione dei dati	Violazione di disponibilità. Messa in atto di misure idonee a contrastare tali eventi	Sistemi Informativi	Al momento della scoperta	Notifica se trattasi di dati personali e se non sono recuperabili da backup
Virus	Violazione di integrità. Messa in atto di misure idonee a contrastare tali eventi	Sistemi Informativi	Al momento della scoperta	Notifica se trattasi di dati personali e se non sono recuperabili da backup o se l'interruzione ha causato disagi agli interessati



TRATTAMENTI INFORMATICI	COSA FARE	CHI DEVE FARLO (Funzionario Segnalante)	QUANDO DEVE FARLO	NOTIFICA
Blackout	Perdita di accesso ai dati. Messa in atto di misure idonee a contrastare tali eventi	SC Tecnico	Al momento della scoperta	Notifica se il periodo di interruzione del servizio ha causato disagi per l'ambito sanitario
Interruzione trasmissione dati su rete	Perdita di accesso ai dati. Messa in atto di misure idonee a contrastare tali eventi	Sistemi Informativi	Al momento della scoperta	Notifica se il periodo di interruzione del servizio ha causato disagi per l'ambito sanitario
Malfunzionamento Centrale Telefonica	Perdita di comunicazione e disagio per gli utenti. Messa in atto di misure idonee a contrastare tali eventi	Sistemi Informativi	Al momento della scoperta	Notifica se il periodo di interruzione del servizio ha causato disagi per l'ambito sanitario
Videosorveglianza	Violazione di riservatezza.	SC Tecnico	Al momento della scoperta	Notifica se trattasi di dati personali
Intrusione dall'esterno	Violazione di riservatezza. Messa in atto di misure idonee a contrastare tali eventi	Sistemi Informativi	Al momento della scoperta	Notifica se l'intrusione ha riguardato dati personali
Malfunzionamento di apparecchiature elettromedicali	Messa in atto di misure idonee a contrastare tali eventi	Ingegneria Clinica	Immediatamente, e in ogni caso entro 12 ore	Notifica se il malfunzionamento ha generato perdita e/o modifica di dati personali
Smarrimento/ Distruzione di un documento contenente dati personali	Violazione di disponibilità. Messa in atto di misure idonee a contrastare tali eventi	Il dirigente della Struttura in cui è avvenuto il furto	Al momento della scoperta	Notifica se trattasi di dati personali e se non sono recuperabili
Accesso non autorizzato ai documenti e divulgazione degli stessi	Violazione di riservatezza. Messa in atto di misure idonee a contrastare tali eventi	Il dirigente della Struttura in cui è avvenuto l'accesso	Al momento della scoperta	Notifica se trattasi di dati personali
Modifica o alterazione dei documenti	Violazione di integrità. Messa in atto di misure idonee a contrastare tali eventi	Il dirigente della Struttura in cui è avvenuto l'accesso	Al momento della scoperta	Notifica se trattasi di dati personali
Consegna di documenti contenenti dati personali a persona diversa dall'interessato	Violazione di riservatezza. Messa in atto di misure idonee a contrastare tali eventi	Il dirigente della Struttura in cui è avvenuto l'accesso	Al momento della scoperta	Notifica se trattasi di dati personali



4. LE DIVERSE FASI



4.1. Scoperta e Qualificazione

Le attività di scoperta dell'incidente, come le successive di trattamento, devono essere documentate, adeguate, tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti, ovvero devono essere chiaramente individuate le violazioni, le circostanze, le conseguenze, e deve essere dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile del trattamento, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare. Ciò significa che nelle situazioni in cui l'Azienda opera come "responsabile del trattamento" (ossia tratta dati personali "per conto" di altre organizzazioni), occorre dare tempestiva notizia della violazione al titolare del trattamento.

4.2. Valutazione

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 la libertà degli interessati.

Si possono distinguere tre tipi di violazioni:

- 1) violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
- 2) violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
- 3) violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

In particolari circostanze le violazioni potrebbero essere combinate tra loro.



Da quanto sopra si ricava che un incidente che determini la non disponibilità di dati per un periodo di tempo deve essere comunque considerato violazione e, dunque, deve essere comunque documentato.

Il Funzionario Segnalante deve determinare i rischi che possono determinare l'obbligo di notifica, in particolare, occorre valutare la possibilità che la violazione possa causare danni fisici, materiali o immateriali alla persona fisica.

A titolo d'esempio: perdita del controllo dei dati personali che li riguardano; limitazione dei loro diritti; discriminazione; furto o usurpazione di identità; perdite finanziarie; decifrazione non autorizzata di un dispositivo; riaccoppiamento non autorizzato di informazioni aggiuntive originariamente disgiunte dai dati personali (rimozione 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.

4.2.1. Come valutare il rischio conseguente a un *data breach*?

La corretta valutazione dei possibili rischi scaturenti da una violazione è un passaggio importante per un'efficiente gestione del *data breach*. L'analisi consente al titolare di individuare con prontezza adeguate misure per arginare o eliminare l'intrusione e di valutare la necessità di attivare le procedure di comunicazione e di notifica (che si ricorda si attivano solo al superamento di determinate soglie di rischio, ovvero, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche).

In particolare, le conseguenze della violazione varieranno a seconda di:

- tipo di violazione e natura dei dati violati (es. violazione di riservatezza, di accessibilità o di integrità dei dati; dati sanitari, documenti di identità);
- facilità con cui potrebbero essere identificati gli interessati (es. se l'aggressione riguarda dati identificativi o dati personali non direttamente identificativi verificare se era previsto l'utilizzo di tecniche di pseudonimizzazione o crittografia);
- gravità delle conseguenze sugli individui in termini di potenziali danni (es. i dati sono stati inviati erroneamente a un fornitore di fiducia o sono stati sottratti da un terzo sconosciuto);
- speciali caratteristiche e numero degli individui interessati (es. bambini o anziani; violazione massiccia o individuale);
- particolari caratteristiche del titolare (es. contatto frequente con dati sensibili).

Accertato il livello di rischio, il titolare sarà in grado di determinare la necessità o meno di eseguire la notifica all'autorità e la comunicazione agli individui interessati.

Per analizzare e valutare l'incidente di sicurezza l'Azienda ha messo a punto la “scheda di incidente di sicurezza” (allegato A).

4.3. Notifica (Art. 33 p.3)

Lo scopo della notifica è di mettere al corrente dell'avvenuta violazione l'Autorità di controllo, e impone al Titolare del trattamento di adottare le misure necessarie a limitare i danni che possono derivare da una violazione dei diritti e libertà degli interessati; l'efficacia di questo dovere di limitazione dipende dalla tempestività e dall'adeguatezza organizzativa e tecnica con cui la violazione è affrontata.

L'obbligo di notifica e quello aggiuntivo di comunicazione devono essere valutati caso per caso in relazione ai diritti ed alla libertà degli interessati.

La Notifica deve:



- a) descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- b) comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati (RPD / DPO) 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 da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Il Funzionario Segnalante può eseguire personalmente la notifica per conto di quest'ultimo. Ciò non toglie che le responsabilità nei confronti dell'autorità e degli interessati scaturenti dalla notifica o dalla sua mancanza, permangano in capo al titolare. Peraltro, in caso di negligenza, il funzionario ne risponderà direttamente nei confronti del titolare.

Se il **Funzionario**, anche quando ha appurato con ragionevole certezza l'esistenza di una violazione, **non** è in possesso di tutti gli elementi utili per effettuare una descrizione completa ed esaustiva dell'infrazione, può utilizzare la tecnica:

- dell'**"approssimazione"**. Il titolare che non sia ancora in grado di conoscere con certezza il numero di persone e di dati personali interessati dalla violazione può comunicarne in prima battuta un ammontare approssimativo, provvedendo a specificare il numero esatto a seguito di accertamenti.
- della **"notificazione in fasi"**. In questo caso il titolare, per la complessità o estensione della violazione, potrebbe non essere in grado di fornire con immediatezza all'autorità tutte le informazioni necessarie. Potrà allora ottemperare agli obblighi di notifica comunicando, dopo una prima e rapida notifica di *alert*, tutte le informazioni per fasi successive, aggiornando di volta in volta l'autorità sui nuovi riscontri.

Infine, è possibile effettuare una notifica differita, dopo le 72 ore previste dall'art. 33 nel caso, per esempio, che l'azienda subisca violazioni ripetute, ravvicinate e di simile natura che interessino un numero elevato di soggetti. Al fine di evitare un aggravio di oneri in capo al titolare e l'invio scaglionato di un numero elevato di notificazioni tra loro identiche, il titolare è autorizzato ad eseguire un'unica "notifica aggregata" di tutte le violazioni occorse nel breve periodo di tempo (anche se superiori le 72 ore), purché la notifica motivi le ragioni del ritardo.

4.3.1. Quando il titolare è ritenuto "a conoscenza" di una violazione?

L'art. 33 impone al titolare di notificare la violazione all'autorità di controllo, ove possibile, **entro 72 ore** dal momento in cui ne viene a conoscenza. Il tempo di riferimento da cui iniziano a decorrere i termini della notifica viene individuato quindi nel momento in cui il titolare acquisisce consapevolezza dell'avvenuta violazione.

Si ritiene che debba considerarsi "a conoscenza" il titolare che abbia un **ragionevole grado di certezza** in merito alla verifica di un incidente di sicurezza. È evidente che, in base alle specifiche circostanze, mentre alcune violazioni saranno facilmente rilevabili, per altre sarà necessario instaurare un'indagine più approfondita. In questi casi, durante la fase di investigazione, il titolare può essere considerato come privo di un grado di conoscenza tale da far scattare immediatamente l'obbligo di notifica. La fase investigativa, non deve comunque essere abusata per prorogare illegittimamente il termine di notifica, in quanto il comportamento del titolare sarà in ogni caso valutato sulla base della sua tempestiva attivazione in caso venga informato di una possibile infrazione.



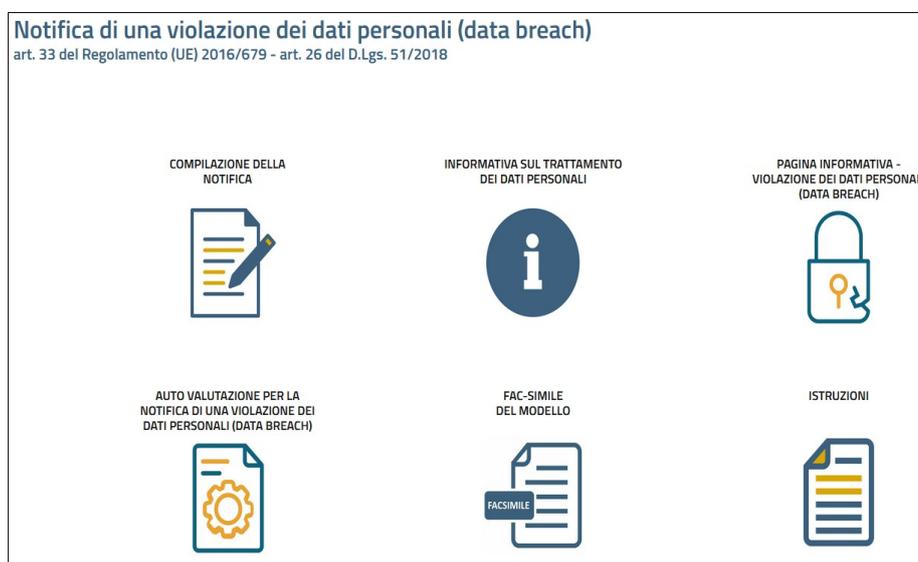
In linea di principio, l’Azienda (titolare del trattamento) si deve considerare a conoscenza della violazione nel momento in cui il proprio funzionario ne sia venuto a conoscenza: non deve perciò esistere alcuna dilazione temporale nelle comunicazioni tra titolare e funzionario segnalante, giacché questi è organico al titolare.

4.3.2. Procedura di notifica

Con il [Provvedimento del 27 maggio 2021 - Procedura telematica per la notifica di violazioni di dati personali \(data breach\) \[9667201\]](#), il Garante ha adottato "un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell’Autorità pubblicato all’indirizzo "<https://servizi.gpdp.it/>", attraverso la quale, a far data dal 1° luglio 2021, i titolari del trattamento forniscono al Garante le informazioni ivi richieste”.

Questa procedura è obbligatoria e sostitutiva del precedente invio a mezzo PEC del modulo.

La procedura è reperibile attraverso il link <https://servizi.gpdp.it/databreach/s/>:



A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite l’apposita procedura telematica, resa disponibile nel portale dei servizi online dell’Autorità.

Nella stessa pagina è disponibile un modello facsimile (**Allegato B**), da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante.

4.3.2.1. Self assessment

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo disposizione un apposito **strumento di autovalutazione (self assessment)** che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

Mediante alcuni semplici quesiti, il titolare viene guidato nell’assolvimento degli obblighi in materia di «**Notifica di una violazione dei dati personali all'autorità di controllo**» (art. 33 del Regolamento (UE) 2016/679 o art. 26 del D.Lgs. 51/2018) e di «**Comunicazione di una violazione dei dati personali all'interessato**» (art. 34 del Regolamento (UE) 2016/679 o art. 27 del D.Lgs. 51/2018). Questo strumento è da considerarsi esclusivamente quale ausilio al processo decisionale del titolare del trattamento e non rappresenta il pronunciamento di questa Autorità sull'applicazione del Regolamento (UE) 2016/679 o del D.Lgs. 51/2018. Le informazioni fornite durante il suo utilizzo non saranno conservate.



Al fine di garantire la correttezza formale, l'uniformità di trattamento nonché consentire la possibilità di effettuare le necessarie operazioni di gestione e monitoraggio delle notifiche delle violazioni dei dati personali, la procedura telematica costituisce l'unica ed ordinaria modalità mediante la quale l'Autorità accoglierà le stesse.

La notifica di una violazione dei dati personali è un adempimento in capo al titolare del trattamento che tipicamente è una persona giuridica, mentre il sistema informatico è strutturato per interagire con una persona fisica. La nuova procedura consente ad una persona fisica - identificata - di effettuare la notifica in nome e per conto del titolare del trattamento previa assunzione della responsabilità, ai sensi dell'art. 168 del Codice, del contenuto della stessa.

Il soggetto che effettua la notifica, pertanto, sarà il rappresentante legale del titolare del trattamento o un'altra persona che agisce su delega dello stesso (utente).

4.3.2.2. Autenticazione

I soggetti muniti di credenziali SPID - livello 2 o in possesso di una nuova carta di identità elettronica (c.d. CIE 3.0), previa autenticazione informatica, potranno accedere al sistema e procedere ad effettuare la notifica di una violazione.

Con le predette modalità di autenticazione, il soggetto che effettua la notifica sarà l'utente che si è autenticato (il cui cognome e nome sarà dedotto a valle della procedura di autenticazione informatica) che dovrà esplicitamente indicare se agisce in qualità di Rappresentante Legale del titolare del trattamento oppure in qualità di soggetto che invia la notifica su delega dello stesso.

Per ampliare le possibilità di utilizzo, il sistema prevede anche la possibilità di sottoscrivere la notifica, in alternativa alle predette modalità, mediante l'apposizione di una firma digitale.

Con questa modalità, l'utente NON autenticato compila il modulo online e riceve una e-mail contenente le istruzioni per completare la procedura. In particolare, sarà necessario:

- 1)** collegarsi ad una specifica pagina web e scaricare il file pdf per prendere visione dei dati forniti durante la compilazione del modulo:
- 2)** sottoscrivere il file pdf di cui al punto precedente con firma digitale (firma elettronica qualificata) in formato CADES-BASELINE-B (estensione p7m) e senza usare "marche temporali".
- 3)** collegarsi ad una specifica pagina web e caricare il file firmato digitalmente e gli eventuali allegati, previo inserimento di un identificativo e di un codice Upload riportati nella e-mail contenente le istruzioni, da utilizzare esclusivamente per le operazioni di caricamento.

Il file caricato al punto 3 sarà analizzato sotto il profilo formale, verificando in particolare la validità della firma digitale e la perfetta corrispondenza fra il file firmato e quello scaricato dalla piattaforma.

Le istruzioni per completare la procedura di notifica saranno inviate via e-mail (posta elettronica ordinaria) all'indirizzo indicato.

L'utente che a fronte della compilazione del modulo online non procede con le operazioni di cui al precedente punto 3 riceverà una e-mail con la quale verrà informato dell'avvenuta cancellazione delle informazioni fornite durante la precedente fase di compilazione.

Nota bene: la procedura di notifica della violazione dei dati personali si intende perfezionata esclusivamente al completamento delle operazioni di cui al punto 3. La mera compilazione del modulo e la conseguente ricezione dell'e-mail contenente le istruzioni non concludono la procedura di notifica della violazione dei dati personali.

4.3.2.3. Compilazione della notifica



L'art. 33, par. 3 del Regolamento, definisce il set minimo di informazioni che il titolare del trattamento deve fornire all'autorità di controllo al momento della notifica di una violazione dei dati personali. Inoltre, l'art. 33, par. 4 del Regolamento, prevede esplicitamente la possibilità in base alla quale "le informazioni possono essere fornite in fasi successive".

Infine, le Linee guida WP 250 suggeriscono che, all'atto della prima notifica all'autorità di controllo, il titolare del trattamento informi quest'ultima del fatto che non dispone ancora di tutte le informazioni richieste e che fornirà ulteriori dettagli in un momento successivo.

Per quanto attiene al dettaglio delle informazioni da fornire, si rinvia al fac-simile del "modello di notifica delle violazioni dei dati personali".

Per semplificare il processo di compilazione nonché i successivi controlli, le informazioni saranno raccolte mediante una serie di domande a cui l'utente è sempre tenuto a rispondere: pertanto, la "mancata risposta" ad una domanda trova esplicita possibilità di espressione previa selezione di specifiche risposte (es. "non ancora determinato", "al momento non si dispone di tali informazioni", ecc.).

Premesso quanto sopra, durante la compilazione della "prima notifica", l'utente deve indicare se si tratta di una notifica "preliminare" o di una notifica "completa".

La qualificazione della "prima notifica" come "preliminare" o "completa" ha esclusivamente la funzione di discriminare l'applicazione dei controlli che garantiscono la presenza del set "minimo" di informazioni che il titolare è tenuto a fornire. A titolo esemplificativo, una notifica in cui il titolare non fornisca informazioni salienti, quali le categorie di dati personali coinvolti, le possibili conseguenze per gli interessati, ecc., non può essere qualificabile come "completa" in quanto priva degli elementi essenziali.

Il titolare ha sempre la facoltà di qualificare una notifica come preliminare qualora ritenga di dover integrare successivamente le informazioni fornite, pur avendo già fornito gli elementi essenziali.

Durante la compilazione di alcune sezioni è possibile indicare la volontà di allegare un file contenente ulteriori informazioni di dettaglio. L'upload degli allegati, sarà consentito al termine della compilazione (nel caso di utenti autenticati) oppure nella fase di upload del file firmato (nel caso di utenti non autenticati). Sono accettati esclusivamente allegati in formato pdf di dimensioni inferiori ai 2,5 MB.

Per agevolare l'utente nella compilazione della notifica, esclusivamente per gli utenti autenticati, è disponibile la funzionalità "Salva in bozza" che consente la compilazione del modulo in fasi successive. Il processo di compilazione deve essere completato entro il termine di 48 ore dal primo salvataggio: trascorso tale termine, i dati inseriti saranno cancellati e dovranno essere nuovamente inseriti.

4.3.2.4. Notifica integrativa

Indipendentemente dalla qualificazione ("preliminare" o di "completa") effettuata dal titolare durante la prima notifica, è sempre garantita la possibilità di integrare una notifica. Il titolare potrebbe "integrare" sia per fornire informazioni ritenute necessarie che mancavano nella prima notifica, o semplicemente perché vuole fornire informazioni aggiuntive di cui è venuto a conoscenza nel tempo.

In tal senso, tenuto conto che in fase di compilazione di una notifica integrativa viene riproposto all'utente il contenuto dell'ultima notifica trasmessa, la notifica integrativa è da intendersi come qualcosa che, previa integrazione o modifica, annulla e sostituisce la precedente.

Per la trasmissione di una notifica integrativa (cfr. sez. B1 del modulo) è necessario far riferimento al numero di fascicolo, e relativo PIN, che la procedura assegna successivamente alla trasmissione della prima notifica.



4.3.2.5. Annullare una notifica

Esclusivamente nei casi in cui, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione, il titolare del trattamento può informarne l'autorità di controllo.

Per questa particolare fattispecie, il titolare può trasmettere una notifica integrativa, selezionando l'opzione d) al punto 1 della Sez. B1, fornendo le motivazioni del caso.

4.3.2.6. Riscontri all'utente e al titolare

Al completamento della procedura di notifica:

- l'utente e il titolare del trattamento riceveranno, rispettivamente all'indirizzo e-mail indicato nella sezione A del modulo e all'indirizzo PEC indicato al punto 2 della sezione C (o all'altro riferimento e-mail, qualora trattasi di soggetto privo di PEC), un documento informatico contenente le informazioni inserite all'atto della notifica;
- l'utente inoltre riceverà una ulteriore comunicazione contenente il numero di fascicolo creato a fronte della trasmissione della prima notifica (preliminare o completa) ed il relativo PIN da utilizzare per trasmettere ulteriori informazioni circa la violazione occorsa avvalendosi della specifica funzionalità per l'invio di "notifiche integrative";

Esclusivamente in caso di notifica effettuata da un utente non autenticato, la notifica può essere rigettata sulla base di alcuni controlli formali (validità della firma, integrità del file trasmesso, ecc.). Il rigetto e la relativa motivazione saranno comunicati esclusivamente all'utente, mediante l'invio di una e-mail all'indirizzo indicato nella sezione A del modulo.

Sulla base delle informazioni acquisite durante la notifica di una violazione dei dati personali, la procedura provvede a classificare la notifica come "DA INTEGRARE" nelle ipotesi in cui la stessa sia stata qualificata come "preliminare" oppure, siano state omesse informazioni essenziali ai fini di una corretta valutazione dei fatti.

In tali circostanze, i titolari saranno destinatari di messaggi automatici con i quali vengono informati, ed esortati, a compiere le dovute azioni successive (l'integrazione) con l'indicazione delle motivazioni. I messaggi saranno inviati, con cadenza periodica fintanto che sussisteranno le condizioni per le quali la notifica è da considerarsi come "DA INTEGRARE".

4.4. Comunicazione della violazione all'interessato (art. 34)

L'art. 34 del GDPR stabilisce che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve comunicare la violazione all'interessato senza ingiustificato ritardo.

L'obbligo di comunicazione risponde allo scopo di consentire all'interessato, qualora sussista una violazione che presenta rischi elevati, di essere informato ed eventualmente prendere le precauzioni necessarie.

La comunicazione dovrebbe essere data direttamente e personalmente agli interessati coinvolti dalla violazione, a meno che ciò comporti 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 la medesima efficacia.

La comunicazione deve essere distinguibile rispetto altre diverse comunicazioni che vengono fatte dal titolare agli interessati: in altri termini, la comunicazione deve essere chiara, inequivocabile e richiamare l'attenzione dell'interessato.

Il rispetto di questi requisiti richiede che il titolare, già prima che si verifichi una causa di comunicazione, considerati i dati che tratta e le categorie di interessati, predisponga un piano specifico di comunicazione.



La comunicazione, pur sussistendo la condizione di rischio elevato, si ritiene soddisfatta quando:

- a) 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;
- b) 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.

Mentre per far scattare l'obbligo di notifica 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 occorre che tale rischio sia elevato.

Il titolare è dunque tenuto non solo ad individuare e qualificare i rischi connessi a violazioni di dati personali ma, qualora tali rischi riguardino i diritti e le libertà delle persone fisiche, deve anche procedere ad una valutazione del livello di rischio.

La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

Criteri per permettere una valutazione accurata:

- 1) Tipo di violazione;
- 2) natura, sensibilità e volume dei dati personali;
- 3) facilità di riconoscimento degli interessati;
- 4) Serietà delle conseguenze per le persone fisiche;
- 5) Caratteristiche specifiche delle persone fisiche;
- 6) Quantità di persone fisiche coinvolte;
- 7) Caratteristiche specifiche del titolare.

Nel caso la segnalazione diretta richieda sforzi sproporzionati, è possibile che questa possa essere effettuata attraverso una comunicazione pubblica. Si sottolinea però che anche questo tipo di comunicazione deve mantenere lo stesso grado di efficacia conoscitiva del contatto diretto con l'interessato.

Allegati:

- A) Scheda di incidente di sicurezza
- B) Modello di notifica all'Autorità
- C) Modello di registro delle violazioni di dati