MINISTERO del LAVORO
e delle POLITICHE SOCIALI

Allegato 7 - Procedura data breach

Linee guida per la gestione delle violazioni di dati personali e la loro eventuale comunicazione all'Autorità e ai soggetti interessati

MINISTERO del LAVORO
e delle POLITICHE SOCIALI

Indice

1. Premessa

Secondo quanto previsto dall'art. 4 («Definizioni») del Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito, "GDPR" o "Regolamento"), per violazione dei dati personali 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*».
In tale contesto, il Regolamento sancisce l'obbligo per il titolare del trattamento di notificare tempestivamente l'avvenuta violazione dei dati personali (c.d. "*Data Breach*") all'autorità di controllo e, in casi determinati e con specifiche modalità, di procedere alla comunicazione direttamente agli interessati.
L'obiettivo del presente documento è disciplinare il processo di gestione delle violazioni di dati personali per il Ministero del lavoro e delle politiche sociali, ossia: definire i principi generali, i ruoli, le responsabilità e le attività da effettuare qualora si verifichi un incidente di sicurezza che comporti la violazione di dati personali.
La presente procedura si applica a tutte le violazioni di dati personali (come di seguito meglio identificate) riscontrate all'interno del Ministero del lavoro e delle politiche sociali.
Le disposizioni del presente documento hanno validità per tutti i dipendenti del Ministero.

2. Definizione di una violazione dei dati personali

Con il termine "violazione dei dati personali" (in inglese "*data breach*") si intende una situazione che può comportare, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso a informazioni qualificate dal Regolamento come dati personali trasmessi, memorizzati o elaborati per mezzo di sistemi informatici o di altra natura.
Coerentemente al Provvedimento n. 157 del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali, la natura della violazione può essere classificata in base ai seguenti principi di sicurezza delle informazioni:

- "perdita di confidenzialità": diffusione, accesso non autorizzato o accidentale;
- "perdita di integrità": modifica non autorizzata o accidentale;
- "perdita di disponibilità": impossibilità di accesso, perdita, distruzione non autorizzata o accidentale.

Di seguito si riportano le principali possibili violazioni di dati personali identificate:

- furto o smarrimento di beni del Ministero, connesso ad un comportamento negligente di dipendenti/collaboratori, che può verificarsi nel caso in cui venga meno il controllo degli strumenti utilizzati per elaborare i dati personali (i.e. Server, PC/laptop, smartphone, device per l'archiviazione di dati esterni);
- accesso illegale da parte di soggetti terzi, ossia accesso abusivo da parte di terzi, non autorizzati, ai sistemi informatici, ad esempio, mediante:
    - un attacco *ransomware*, mirato al furto di documenti. Questo tipo di attacco di solito può essere classificato come violazione della disponibilità dei dati personali, ma spesso potrebbe verificarsi anche una violazione della riservatezza degli stessi;

  - attacchi *injection* (*SQL injection, path traversal*). Tali attacchi mirano a copiare e abusare dei dati personali. Si tratta principalmente di violazioni della riservatezza, ma spesso potrebbe verificarsi anche una violazione dell'integrità degli stessi;
  - attacchi *phising*, ossia truffe informatiche effettuate inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati, motivando tale richiesta con ragioni di ordine tecnico. Tali attacchi sono classificati come violazioni della riservatezza dei dati personali;
- errore accidentale da parte di uno dei soggetti che trattano dati personali (i.e. invio di una mail contenente dati personali ad un destinatario errato);
- furto di informazioni, può verificarsi nel caso in cui un dipendente (o ex dipendente) sfrutti la propria conoscenza o le proprie autorizzazioni per sottrarre dolosamente dati/informazioni di carattere personale;
- vigilanza/adozione di misure di sicurezza, qualora, a causa di un'erronea valutazione sul livello di criticità dei dati e/o informazioni ministeriali, non siano state poste in essere le necessarie precauzioni volte alla salvaguardia dei dati medesimi, che sono stati perduti.

3. Ruoli e responsabilità

Coerentemente con il modello organizzativo in ambito privacy adottato dal Ministero del lavoro e delle politiche sociali declinato nel D.M. n. 37 del 10 aprile 2019, si riportano i ruoli e le responsabilità di ciascuna figura coinvolta nel processo di gestione e segnalazione delle violazioni:

- Soggetto che esercita le funzioni di titolare del trattamento: dopo aver valutato la portata e il livello di rischio della avvenuta violazione di dati personali, si occupa di individuare e adottare possibili misure di rimedio e, ove necessario, di notificare la violazione all'autorità di controllo competente entro 72 ore dal momento in cui ne è venuto a conoscenza, salvo che si riveli improbabile che la violazione medesima possa presentare un rischio per i diritti e le libertà delle persone fisiche. Comunica la violazione agli interessati, qualora la stessa sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Prevede attività di verifiche periodiche volte a garantire l'efficacia delle procedure e degli strumenti di risposta agli incidenti relativi alle violazioni di dati personali;
- Responsabile della protezione dei dati: funge da punto di contatto tra il titolare, il Garante e gli interessati; nell'ambito della gestione degli incidenti, raccoglie tutte le possibili violazioni di dati personali e individua il soggetto che esercita le funzioni di titolare che sarà competente per la gestione della eventuale violazione. Avvalendosi della collaborazione delle risorse a sua disposizione e dei referenti privacy, può essere consultato dal soggetto che esercita le funzioni di titolare nell'attività di valutazione della avvenuta violazione di dati e nella gestione dei rapporti con il Garante. Il RPD ha una funzione di consulenza e supporto, non potendosi in alcun caso sostituire al soggetto che esercita le funzioni di titolare nell'assolvimento dei compiti e nelle decisioni che spettano a quest'ultimo, salva diversa disposizione di legge;

- Referente privacy: svolge attività di supporto al soggetto che esercita le funzioni di titolare per le questioni relative alla tutela dei dati personali trattati e rappresenta il punto di contatto con il RPD. In tale veste, il referente si occupa di:
    - raccogliere le segnalazioni di potenziali data breach, ricevute dal RPD, ovvero da qualsiasi altra fonte esterna o interna, e di trasmettere immediatamente le stesse al responsabile interno coinvolto;
    - coadiuvare il responsabile interno e colui che esercita le funzioni di titolare nella valutazione della segnalazione;
    - tenere e aggiornare il registro delle violazioni (all. 1), secondo le istruzioni illustrate nel prosieguo;
    - supportare il RPD qualora il soggetto che esercita le funzioni di titolare abbia richiesto il suo intervento, anche attraverso la messa a disposizione in suo favore di tutti gli elementi valutativi necessari l'espletamento dei suoi compiti.
- Responsabile interno del trattamento: in qualità di dirigente a capo dell'unità organizzativa dove si è verificata la violazione, supporta il soggetto che esercita le funzioni di titolare del trattamento nella gestione della violazione dei dati, svolgendo le seguenti attività:
    - adotta le misure di sicurezza tecnico/organizzative previste dalla normativa interna;
    - coordina le attività degli autorizzati al trattamento e si interfaccia con gli Amministratori di Sistema;
    - ove ritenga che l'incidente occorso possa aver comportato una violazione dei dati personali, informa senza ritardo il soggetto che esercita le funzioni di titolare del trattamento;
    - fornisce, con l'ausilio degli autorizzati al trattamento, degli Amministratori di Sistema, e dei referenti privacy, elementi utili all'esercente le funzioni di titolare per l'eventuale predisposizione delle eventuali comunicazioni da trasmettere al Garante privacy e agli interessati.
- Autorizzati: soggetti preposti materialmente ad una o più attività di trattamento che coadiuvano il responsabile interno/esterno del trattamento coerentemente con le responsabilità attribuitegli, svolgendo le seguenti attività:
    - comunicano eventuali violazioni di dati personali di cui sono a conoscenza mediante l'invio di una comunicazione da inviare agli altri appositi strumenti e canali messi a disposizione dal Ministero;
    - forniscono supporto in fase identificazione dell'incidente, comunicando ai responsabili interni del trattamento informazioni utili per la classificazione delle violazioni verificatesi.
- Amministratori di Sistema (di seguito anche "AdS"): soggetti che, in qualità di preposti alle attività di gestione e manutenzione dei sistemi informatici ministeriali, coadiuvano il responsabile interno del trattamento, coerentemente con le responsabilità attribuitegli, svolgendo le seguenti attività:
    - monitorano i sistemi di sicurezza;
    - comunicano in caso di violazione tutte le informazioni necessarie alla sua comprensione e le trasmettono ai responsabili interni ed esterno del trattamento;

- comunicano le eventuali azioni poste in essere per la gestione della violazione ai responsabili interno ed esterno del trattamento e al RPD;
- monitorano nel continuo le attività necessarie a prevenire eventuali violazioni/ e le attività che rilevino le eventuali non conformità delle misure di sicurezza;
- comunicano ai responsabili interni ed esterni del trattamento e al RPD eventuali situazioni che potrebbero comportare violazioni di dati personali;
- raccolgono le informazioni per quanto di competenza, necessarie a formulare compiutamente le comunicazioni verso il Garante /Interessato.

4. Riferimenti

Di seguito l'elenco dei **documenti** che costituiscono il **riferimento** per le presenti linee guida:

- Regolamento UE n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla protezione dei dati);
- D.Lgs. n. 196/03 Codice in materia di protezione dei dati personali e successive modifiche e integrazioni;
- D.M. n. 37 del 10 aprile 2019, recante "*Direttiva per la individuazione dei soggetti tramite i quali il Ministero del lavoro e delle politiche sociali esercita le funzioni di titolare del trattamento, ai sensi del regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*" in cui sono stati declinati i ruoli e le responsabilità in ordine agli adempimenti previsti in capo al Ministero del lavoro quale titolare del trattamento dei dati personali, nel complesso delle sue articolazioni organizzative;
- Linee guida in materia di notifica delle violazioni di dati personali (*data breach notification*) – WP 250, adottate dal Gruppo di lavoro Art. 29 il 06 febbraio 2018;
- Provvedimento n. 157 del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali;
- Linee guida in materia di notifica delle violazioni di dati personali (*Examples regarding Data Breach Notification*), adottate *dall'European Data Protection Board* il 14 gennaio 2021;
- Provvedimento n. 209 del Garante del 27 maggio 2021 sulla Procedura telematica per la notifica di violazioni di dati personali (*data breach*).

5. Procedura di data breach

La procedura di *data breach* adottata dal Ministero del lavoro e delle politiche sociali è articolata nelle fasi riportate all'interno dei seguenti diagrammi di flusso:

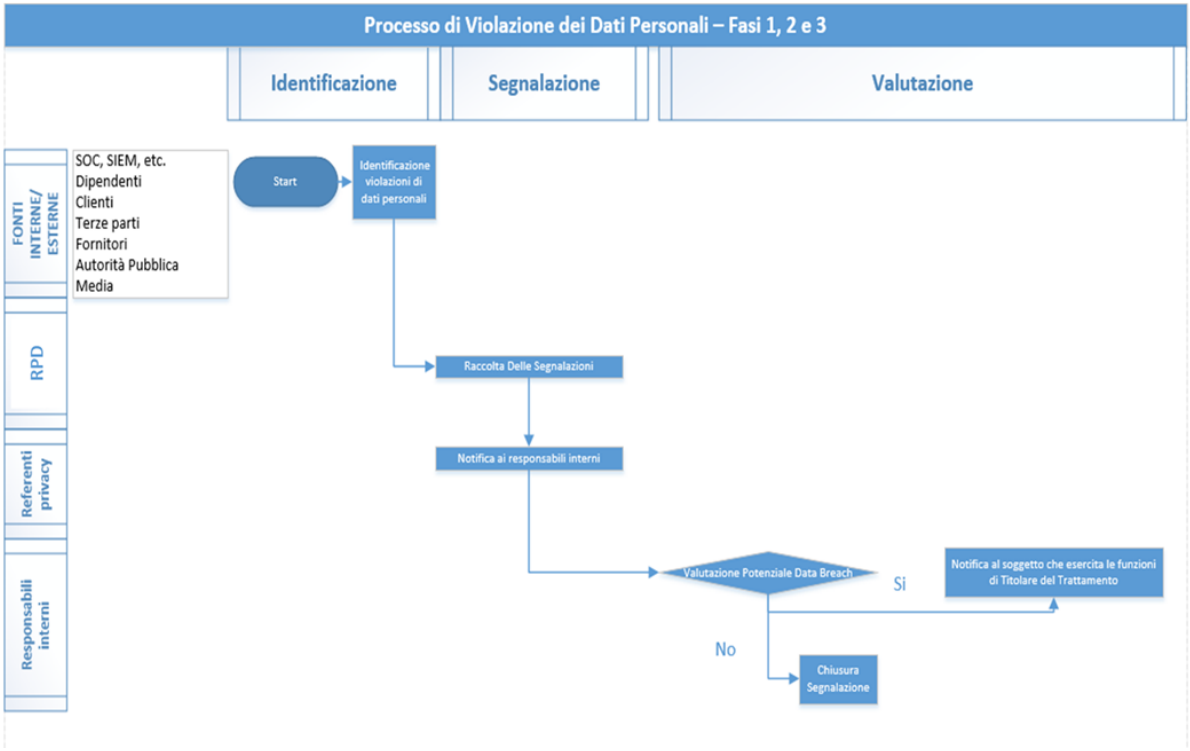

Figura 1 – Procedura di data breach fasi 1-2-3

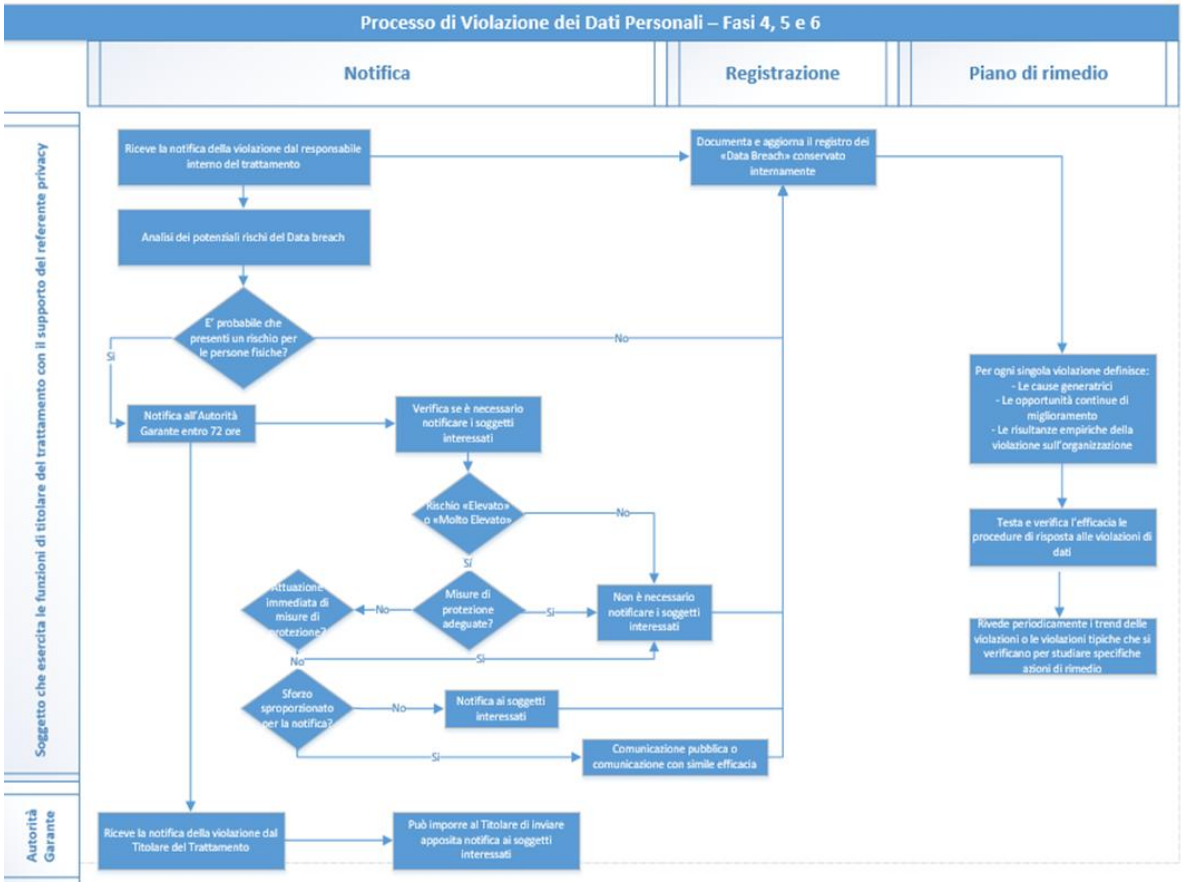

Figura 2 – Procedura di data breach fasi 4-5-6

Di seguito si riporta la descrizione delle attività previste per ciascuna fase del processo di data breach.

6. Identificazione di un potenziale data breach

La fase di identificazione di una violazione di dati personali ha l'obiettivo di rilevare un potenziale *data breach* derivante dalla perdita, divulgazione non autorizzata, trattamento illecito e/o perdita di disponibilità di dati personali di cui il Ministero del lavoro e delle politiche sociali è titolare.
Tutte le possibili violazioni dei dati personali devono essere identificate e indirizzate tempestivamente al Responsabile della protezione dei dati. Le segnalazioni possono provenire da fonti interne e fonti esterne al Ministero, quali:

- Strumenti informatici di monitoraggio di eventi di sicurezza (es. Microsoft Azure) o attraverso misure tecniche di sicurezza finalizzate alla protezione dei sistemi informativi;
- Dipendenti/autorizzati al trattamento;
- Cittadini;
- Fornitori e terze parti;

- Autorità di vigilanza;
- Media (es. stampa, telegiornali, agenzie di informazione multimediale, ecc.).

Ogni soggetto che presta la propria attività a favore del Ministero del lavoro e delle politiche sociali, che venga a conoscenza o sospetti che sia avvenuta una violazione di dati personali, deve darne immediata comunicazione tramite invio di una mail all'indirizzo *gdpr@lavoro.gov.it*. La comunicazione deve contenere un'indicazione chiara dell'evento verificatosi, delle caratteristiche dei dati personali coinvolti e, ove possibile, dell'unità organizzativa interessata dalla violazione.
Il competente Responsabile della protezione dei dati, una volta ricevuta la comunicazione sul potenziale *data breach*, individua il soggetto che esercita le funzioni di titolare che sarà competente per la gestione della eventuale violazione e trasmette senza ritardo la comunicazione ai referenti privacy della struttura individuata.
Il referente privacy inoltra la comunicazione pervenuta al responsabile o ai responsabili interni e collabora con gli stessi nell'attività di valutazione del livello e delle potenzialità di rischio per gli interessati dell'evento descritto nella comunicazione.
Qualora la presunta violazione inerisca a dati personali trattati da un responsabile esterno, sarà dovere dello stesso rilevarla e darne comunicazione al Ministero con cui ha contrattualizzato il rapporto professionale. Pertanto, indipendentemente dal canale di comunicazione, il processo si attiva con l'avvenuto ricevimento della segnalazione al responsabile esterno.

7. Esecuzione dei riscontri interni

Il responsabile interno del trattamento interessato, ricevuta la comunicazione della presunta violazione di dati personali, effettua alcune verifiche interne volte a vagliarne l'attendibilità. Al fine di condurre una valutazione sulla presunta violazione, il responsabile si potrà avvalere dell'ausilio del tool di autovalutazione messo a disposizione dei titolari del trattamento dal Garante per la Protezione dei Dati personali e reperibile al seguente link https://servizi.gpdp.it/databreach/s/self-assessment. Il *tool* supporterà il responsabile nel valutare se dall'incidente di sicurezza occorso si sia verificata una violazione dei dati personali.
Nell'ambito di tali verifiche, con l'ausilio dei referenti privacy, nonché avvalendosi della collaborazione degli autorizzati al trattamento e degli amministratori di sistema, il responsabile interno esegue con urgenza i riscontri preliminari e, in caso di esito positivo, comunica al soggetto che esercita le funzioni di titolare e al RPD l'avvenuta violazione, con specifica indicazione delle seguenti informazioni, ove disponibili:

- la Direzione coinvolta;
- la data dell'evento e l'ora della violazione anche solo presunta (specificando se è presunta);
- la data e ora in cui si è avuto conoscenza della violazione;
- la fonte di segnalazione;
- la natura dell'evento anomalo;
- una sintetica descrizione dell'evento anomalo;
- il numero e la categoria di interessati coinvolti;

- la categoria e il volume di dati personali di cui si presume la violazione;
- la descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione;
- indicazione dell'eventuale Responsabile esterno del trattamento coinvolto nella gestione del sistema informatico;
- Misure di sicurezza adottate al set di dati oggetto di violazione;
- Misure proposte per la mitigazione della presunta violazione;
- Esito della autovalutazione condotta mediante il *tool* messo a disposizione dal Garante per la Protezione dei Dati Personali.

La comunicazione del responsabile interno è effettuata utilizzando l'apposita scheda dell'evento e comunicata tramite mail al RPD e all'esercente le funzioni di titolare l'avvenuta compilazione della scheda (all. 2).
Qualora la violazione sia stata riscontrata dal responsabile esterno, le verifiche del caso saranno poste in essere dal responsabile medesimo, che provvederà a darne tempestiva comunicazione tramite mail al soggetto che esercita le funzioni di titolare del trattamento e al RPD.
Dal momento della ricezione di tale comunicazione da parte del soggetto che esercita le funzioni di titolare del trattamento, ovvero "Tempo zero – T0", decorrono le tempistiche previste dal Regolamento per la gestione degli adempimenti connessi alle violazioni accertate.

8. Valutazione e mitigazione

Il soggetto che esercita le funzioni di titolare del trattamento, ricevuta la comunicazione della violazione, valuta la complessità della stessa, basandosi sulle informazioni ricevute dal responsabile e provvede ad aggiornare la scheda evento, avvalendosi della collaborazione del referente privacy.

La violazione è definita complessa quando:

- i dati personali sono di carattere sensibile/particolare e/o di natura finanziaria;
- i sistemi informatici oggetto di violazione sono complessi per qualità/quantità di informazioni elaborate;
- comprende le chiavi di accesso/cifratura in possesso degli interessati (i.e. password).

Nel caso in cui non ricorrano le caratteristiche di cui sopra, ossia qualora i sistemi informativi coinvolti siano limitati e/o protetti da misure adeguate (es. cifratura), o qualora non siano coinvolti interessati, se non in numero limitato e i dati personali siano parziali e non associati ad altre informazioni (es. nome e cognome senza codice fiscale o carta di credito o numeri telefonici), la violazione può essere definita non complessa.
In questa fase, si raccomanda al soggetto che esercita le funzioni di titolare del trattamento, in caso di dubbi sulla valutazione, di scegliere lo scenario di maggior tutela per gli interessati.
Per ciascuna violazione dei dati personali, devono essere identificate opportune misure correttive tecniche e organizzative da adottare, al fine di mitigare i relativi effetti e ridurre la probabilità di impatto e ricorrenza.
Le misure di mitigazione dovranno essere adeguate alla natura della violazione dei dati personali.

È preferibile che nelle attività di valutazione dell'evento e di individuazione di misure di mitigazione e di rimedio l'esercente le funzioni di titolare si avvalga della consulenza e del supporto tecnico del responsabile della protezione dei dati.
Nell'ipotesi in cui risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, ossia la violazione sia stata ritenuta non complessa, il soggetto che esercita le funzioni di titolare del trattamento non è tenuto a notificare la violazione all'Autorità Garante, pur restando fermo il dovere di censire il *data breach* all'interno del registro delle violazioni.

9. Notifica all'Autorità Garante

L'esercente le funzioni di titolare del trattamento si avvarrà del supporto del tool messo a disposizione dei titolari del trattamento dal Garante per la Protezione dei Dati personali e reperibile al seguente link https://servizi.gpdp.it/databreach/s/self-assessment, al fine di verificare se la violazione occorsa possa rappresentare un rischio per i diritti e le libertà degli interessati. Il tool supporterà il soggetto che esercita le funzioni di titolare nell'individuazione delle azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.
Qualora risulti probabile che il *data breach* possa rappresentare un rischio per i diritti e le libertà degli interessati, ossia la violazione sia stata ritenuta complessa, il soggetto che esercita le funzioni di titolare del trattamento è tenuto a notificare l'avvenuta violazione di dati personali all'Autorità Garante entro 72 ore dal T0, di cui al paragrafo 2.
In questa fase è necessario coinvolgere il responsabile della protezione dei dati, che, è chiamato a esprimere un parere circa la necessità e l'opportunità di notificare l'avvenuta violazione all'Autorità Garante e di comunicare la stessa agli interessati, senza ritardo, stante la necessità di notificare la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il titolare del trattamento è venuto a conoscenza della violazione. A tale scopo, il RPD, con l'ausilio dei referenti privacy, ha la facoltà di svolgere ulteriori riscontri necessari a completare le evidenze mancanti rispetto alle prime analisi condotte. Qualora esprima un parere, il RPD è tenuto ad aggiornare l'apposita scheda evento di cui sopra.
Il soggetto che esercita le funzioni di titolare del trattamento, ricevuto il parere del RPD, invia la comunicazione all'Autorità Garante entro e non oltre le 72 ore dal T0 tramite l'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/.
Il parere del RPD non ha carattere né obbligatorio né vincolante, sicché l'esercente le funzioni di titolare è tenuto, in ogni caso, a notificare la violazione al Garante ogni qual volta lo ritenga opportuno, motivando le sue valutazioni all'interno dell'apposita scheda evento.
I tempi di notifica, nonché l'oggetto delle comunicazioni inviate al Garante devono essere formalizzati all'interno del registro delle violazioni.
Nelle ipotesi in cui il soggetto che esercita le funzioni titolare versi nel dubbio circa la complessità del *data breach* e ritenga necessari ulteriori riscontri, oltre il termine di 72 ore dal T0, è tenuto a comunicare comunque gli estremi della violazione all'Autorità Garante, indicando nella notifica stessa le informazioni in

suo possesso e il termine entro il quale si ritiene termineranno le ulteriori attività istruttorie. Una volta compiute le verifiche necessarie, dovrà essere inviata una seconda comunicazione al Garante, in cui verranno illustrati gli esiti dei successivi riscontri effettuati e le valutazioni compiute in ordine alle conseguenze e ai potenziali rischi dell'avvenuta violazione.

10. Comunicazione agli interessati

Al fine di valutare se la violazione occorsa possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'esercente le funzioni di titolare del trattamento si avvarrà del supporto del *tool* messo a disposizione dei titolari del trattamento dal Garante per la Protezione dei Dati personali e reperibile al seguente link https://servizi.gpdp.it/databreach/s/self-assessment.
Qualora l'esito della valutazione rappresenti che la violazione dei dati personali è suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, il soggetto che esercita le funzioni di titolare del trattamento, con il supporto del RPD, predispone la comunicazione agli interessati e la trasmette al Segretario Generale. Quest'ultimo comunica la violazione all'interessato, o agli interessati, senza ingiustificato ritardo, utilizzando i canali ufficiali di comunicazione a disposizione del Ministero.
Qualora la comunicazione risulti necessaria, saranno adottate le seguenti misure:

- Il Segretario Generale, previa consultazione con il RPD e in coordinamento con quest'ultimo, comunica la violazione agli interessati, entro 5 giorni dalla scoperta della violazione;
- La comunicazione avviene preferibilmente su base individuale per e-mail, salvo che sia impossibile procedere in tal modo, nel qual caso la comunicazione viene effettuata tramite il sito internet del Ministero e/o tramite pubbliche affissioni nelle sedi ministeriali e/o tramite messaggi *push* inviati da app ad uso interno od esterno, ove disponibili;
- La comunicazione all'interessato deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le seguenti informazioni:
    - una descrizione della natura della violazione;
    - il nome e i dati di contatto del RPD o di altro punto di contatto;
    - una descrizione delle probabili conseguenze della violazione;
    - una descrizione delle misure adottate o di cui si propone l'adozione da parte del Ministero per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Si rammenta che, ai sensi dell'art. 34, par. 3 del Regolamento, non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

1) il soggetto che esercita le funzioni di 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;
2) il soggetto che esercita le funzioni di titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

3) 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.

Nel caso in cui il soggetto che esercita le funzioni di titolare del trattamento abbia deciso di non comunicare la violazione di dati personali agli interessati, deve far menzione all'interno del registro delle violazioni delle ragioni a fondamento della propria decisione. In tal caso, l'Autorità di controllo, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà degli interessati, può chiedere che colui che esercita le funzioni di titolare provveda alla comunicazione ovvero può ritenere che una delle condizioni più sopra menzionate sia soddisfatta.

11. Aggiornamento del registro delle violazioni

Il soggetto che esercita le funzioni di titolare del trattamento, con il supporto dei referenti privacy, una volta terminate le fasi precedenti, procede all'aggiornamento del registro delle violazioni. Segnatamente, il registro dovrà contenere le seguenti informazioni:

a) Codice Identificativo *data breach*;
b) Data in cui è avvenuta la violazione;
c) Data, orario e modalità in cui si è avuta conoscenza della violazione;
d) Natura e causa della violazione;
e) Descrizione del *data breach*;
f) Categoria di interessati coinvolti;
g) Numero di interessati coinvolti (anche approssimativo);
h) Categoria di dati personali coinvolti;
i) Numero di dati personali coinvolti (anche approssimativo);
j) Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione;
k) Misure di sicurezza tecniche e organizzative adottate al momento della violazione;
l) Responsabili esterni del trattamento coinvolti, ove applicabile;
m) Possibili conseguenze della violazione sugli interessati;
n) Potenziali effetti negativi per gli interessati;
o) Azioni intraprese in risposta all'incidente per mitigare il danno e ridurre la probabilità di una recidiva simile;
p) Stima della gravità della violazione;
q) Indicazione dell'avvenuta notifica all'Autorità Garante (nei casi in cui non si sia proceduto con tale notifica, è necessario specificarne le ragioni);
r) Comunicazione della violazione agli interessati (ove necessario);
s) Numero di interessati a cui è stata comunicata la violazione;
t) Canale utilizzato per la comunicazione agli interessati;

u) Eventuale notifica ad altre autorità di controllo, organismi di vigilanza o di controllo o all'autorità giudiziaria o di polizia.

12. Definizione del piano di rimedio

Una volta concluso il processo di notifica e comunicazione della violazione di dati personali agli interessati, il soggetto che esercita le funzioni di titolare del trattamento, supportato dal RPD, svolge le seguenti attività:

- Analizza le cause che hanno determinato la violazione di dati personali;
- Valuta le opportunità di miglioramento dei presidi e dei processi di monitoraggio delle violazioni dei dati personali, al fine di mettere in atto misure tecniche e organizzative adeguate a garantire il rispetto del Regolamento;
- Definisce un piano di rimedio al fine di garantire un livello di sicurezza adeguato ai rischi in ordine alla protezione dei dati personali trattati.

Per ciascuna violazione di dati personali, l'esercente le funzioni di titolare del trattamento è tenuto a verificare se l'incidente è il risultato di un errore umano o di un problema di natura tecnica o organizzativa e valutare misure correttive volte a prevenire il ripetersi dell'evento. È, altresì, necessario che il soggetto che esercita le funzioni di titolare del trattamento preveda attività di verifica periodiche volte a garantire l'efficacia delle procedure e degli strumenti di risposta agli incidenti relativi alle violazioni di dati personali.
L'esercente le funzioni di titolare del trattamento, insieme ai responsabili interni di riferimento e con il supporto del RPD, deve periodicamente monitorare quelle violazioni che hanno maggiore probabilità di verificarsi, in modo da applicare azioni correttive specifiche a fronte delle situazioni rilevate. In merito all'esito di tali test, qualora gli stessi evidenzino dei gap procedurali/organizzativi o tecnici, è opportuno che il RPD, con la collaborazione dei referenti privacy, identifichi azioni ed interventi di rimedio da sottoporre al soggetto che esercita le funzioni di titolare del trattamento.

Obblighi di comunicazione del Ministero quando opera in qualità di responsabile del trattamento

Quando il Ministero agisce in qualità responsabile del trattamento, in caso di violazione dei dati personali deve informare il titolare del trattamento, senza ingiustificato ritardo secondo i tempi e i modi concordati negli accordi per il trattamento dei dati personali.

Allegati

- All. 1: Registro delle violazioni;
- All. 2: Scheda dell'evento.

Allegato 1 - Registro delle violazioni

All'interno del Registro delle violazioni sono contenute le seguenti informazioni:

- Codice data breach
- Data in cui è avvenuta la violazione
- Data, orario e modalità in cui si è venuti a conoscenza della violazione
- Natura della violazione
- Causa della violazione
- Descrizione data breach
- Categoria di interessati coinvolti
- Numero di interessati coinvolti (anche approssimativo)
- Categoria di dati personali coinvolti
- Numero di dati personali coinvolti (anche approssimativo)
- Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente
- Misure di sicurezza tecniche e organizzative adottate al momento della violazione
- Responsabili Esterni del Trattamento Coinvolti (Se Applicabile)
- Possibili conseguenze della violazione sugli interessati
    - In caso di perdita di confidenzialità
    - In caso di perdita di integrità
    - In caso di perdita di disponibilità
- Potenziali effetti negativi per gli interessati
- Stima della gravità della violazione
- Azioni intraprese in risposta all'incidente
- Notifica al Garante
- Se NO, specificare le ragioni
- Data della notifica al Garante
- Comunicazione all'interessato
- Se no, specificare le ragioni
- Numero di interessati a cui è stata comunicata la violazione
- Canale utilizzato per la comunicazione agli interessati
- Data della comunicazione all'interessato
- Specificare se la notifica è stata inviata ad altre autorità di controllo, organismi di vigilanza o di controllo o all'autorità giudiziaria o di polizia
- Eventuali note

Allegato 2 – Scheda dell'evento

All'interno della scheda dell'evento sono contenute le seguenti informazioni:

- Direzione coinvolta
- Data evento e ora della violazione anche solo presunta (specificando se è presunta)
- Data e ora in cui si è avuto conoscenza della violazione
- Fonte di segnalazione
- Natura dell'evento anomalo
- Descrizione dell'evento anomalo
- Numero e categoria di interessati coinvolti
- Categoria e volume dei dati personali di cui si presume la violazione
- Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione
- Eventuale Responsabile esterno del trattamento coinvolto nella gestione del sistema informatico
- Misure di sicurezza adottate al set di dati oggetto di violazione
- Misure proposte per la mitigazione della presunta violazione
- Parere dell'RPD in merito al livello di rischio del data breach e all'opportunità di notificarlo al garante/ comunicarlo agli interessati
- Valutazione del soggetto che esercita le funzioni di titolare in merito al livello di rischio del data breach e all'esigenza di notifica al garante/ comunicazione agli interessati