PROCEDURA DI GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI

Sommario

1. Premessa

Per "Data Breach" si intende una "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, par.1, punto 12 del GDPR).

L'Art. 33 del GDPR recita che "*in caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'Art. 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*". La mancata notifica può comportare ulteriori accertamenti da parte dell'Autorità di controllo poiché può rappresentare un indizio di carenze che, se accertate, possono dar luogo a sanzioni.

Con il provvedimento del Garante sulla notifica delle violazioni dei dati personali (30 luglio 2019) è stato predisposto un modello al fine di adempiere più agevolmente all'obbligo di notifica, *ex* art. 33 GDPR. Tutti gli eventi di Data Breach, compresi quelli per cui non sono necessarie le notifiche, devono essere documentati (Art. 33, par. 5, del GDPR) nel registro dei Data Breach.

È, pertanto, necessaria una specifica attenzione dell'Azienda nel predisporre misure tecniche e organizzative adeguate che garantiscano la tutela dei dati personali e prevengano la violazione dei dati personali c.d. "Data Breach".

A seguito di incidente di sicurezza e/o sospetta/presunta violazione di dati personali, le strutture aziendali coinvolte devono, nell'ambito delle loro competenze, predisporre i mezzi e gli strumenti tecnologici ed organizzativi per:

- individuare la violazione o sospetta violazione;
- analizzare le cause della violazione;
- definire le misure da adottare per rimediare alla violazione dei dati personali e attenuarne i possibili effetti negativi;
- registrare le informazioni relative alla violazione;
- rispondere alle potenziali violazioni dei dati, coinvolgendo anche i fornitori;
- fornire consulenza specialistica nel settore di competenza in supporto ai soggetti identificati come riceventi.

2. Scopo

Scopo della presente procedura è descrivere le azioni da intraprendere in caso di una violazione o sospetta violazione dei dati personali (Artt. 33-34 GDPR), ponendo particolare attenzione affinché siano effettuati tutti gli adempimenti al fine di evitare/limitare i danni e consentire che siano rispettati i tempi richiesti per la segnalazione all'Autorità di controllo.

3. Area di applicazione

La procedura è applicata dal Gruppo Data Breach, costituito dalle seguenti strutture/figure:

- DPO;
- Affari Generali;
- Tecnologie informatiche;

- Direttore/Dirigente/Referente Privacy della struttura coinvolta.

4. Acronimi e abbreviazioni

Nel documento sono utilizzati i seguenti acronimi:

- AgID: Agenzia per l'Italia Digitale;
- DPO: Data Protection Officer;
- GDPR: General Data Protection Regulation;
- PEC: Posta Elettronica Certificata;
- ARCS: Azienda Regionale di Coordinamento per la Salute.

5. PROCEDURA

5.1. Attivazione

La procedura viene attivata da chiunque venga a conoscenza o sospetti un incidente di sicurezza e/o violazione di dati personali.

La segnalazione può, pertanto, pervenire da:

- canali interni:
  - da chiunque all'interno dell'Azienda rilevi/sospetti una violazione di dati personali (nel caso di specie, il personale interno all'azienda provvede a comunicare il sospetto incidente direttamente al proprio Direttore/Dirigente/Referente Privacy della struttura coinvolta);
  - dal DPO in quanto punto di contatto primario per gli interessati (nel caso di specie, il DPO provvede direttamente ad informare il Gruppo Data Breach per gli adempimenti conseguenti);
  - dal personale dell'ufficio Tecnologie Informatiche di ARCS nel caso in cui un incidente di sicurezza informatica comporti una violazione di dati personali (in caso di specie, il sospetto indicente va comunicato direttamente al DPO aziendale);
- canali esterni (la comunicazione va effettuata sempre al DPO aziendale, a mezzo dei canali previsti):
  - segnalazione dell'interessato;
  - segnalazione da parte dei fornitori;
  - segnalazione da parte di ulteriori soggetti;
  - segnalazione da parte degli Organi Pubblici (AgID, Polizia, altre Forze dell'Ordine, giornalisti, ecc.).

In questa prima fase devono essere attuate le prime azioni per il contenimento dell'incidente. A titolo esemplificativo: in caso di accesso non autorizzato ai sistemi è consigliato cambiare la password di accesso; in caso di perdita dei dati è necessario verificare se sono stati effettuati dei back up al fine di ripristinare al più presto i dati; in caso di furto di documentazione occorre verificare che siano state messe in atto opportune misure di sicurezza come la chiusura a chiave di una stanza o la presenza di un lucchetto.

5.2. Dati di contatto del Gruppo Data Breach

Ruolo	Indirizzo e-mail	Numero di telefono
DPO	rpd@arcs.sanita.fvg.it	335/1302371
Affari Generali	affari.generali@arcs.sanita.fvg.it	0432/1438030
Tecnologie Informatiche	tecnologie.informatiche@arcs.sanita.fvg.it	0432/1438100

5.3. Input e Output

Le informazioni di avvio della procedura sono:

- segnalazione di violazione o presunta violazione di dati personali (Data Breach);
- registro dei Data Breach.

Le informazioni che escono, quali output della procedura, sono:

- notifica (eventuale) all'Autorità di Controllo;
- comunicazione (eventuale) all'Interessato;
- comunicazione al Titolare del trattamento;
- registro dei Data Breach aggiornato.

5.4. Identificazione dei ruoli

A seguito di comunicazione di sospetto incidente/violazione da parte del personale dipendente ARCS, il Direttore/Dirigente/Referente Privacy della struttura coinvolta provvede a compilare il modulo (v. allegato A) e a trasmettere il medesimo, senza ritardo alcuno, all'indirizzo rpd@arcs.sanita.fvg.it.

All'atto di ricevimento della segnalazione, il DPO provvede ad informare immediatamente il Gruppo Data Breach.

Costituito il Gruppo Data Breach, i presenti procedono con l'analisi preliminare volta a raccogliere tutte le informazioni relative all'evento segnalato:

- data e ora;
- fonte;
- tipologia dell'evento e descrizione;
- stima del numero interessati coinvolti;
- stima della numerosità dei dati personali di cui si presume la violazione;
- luogo in cui è avvenuta la violazione o presunta violazione;
- descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

Nel caso in cui la segnalazione pervenuta riguardi trattamenti di dati personali svolti dall'Azienda in qualità di Responsabile, si procede come descritto al paragrafo 5.11. "Gestire la segnalazione in qualità di Responsabile".

Nel caso in cui la segnalazione pervenuta riguardi trattamenti di dati personali svolti dall'Azienda in qualità di Titolare si procede con i passi seguenti.

5.5. Analisi di primo livello

Una volta raccolte le informazioni di cui al punto precedente, il Gruppo Data Breach procede con l'analisi di primo livello.

L'analisi di primo livello ha come obiettivo quello di verificare che la segnalazione non sia un falso positivo, ovvero l'evento non abbia comportato la violazione di dati personali.

Nel caso in cui l'evento segnalato risulti un falso positivo, verrà comunque tenuta traccia dell'episodio a mezzo di compilazione del registro delle violazione da parte della struttura Affari Generali.

Nel caso in cui la violazione dei dati personali venga accertata, il Gruppo Data Breach passa alla fase di analisi di secondo livello.

5.6. Analisi di secondo livello

Nell'ipotesi in cui venga accertata la violazione dei dati personali (v. allegato B), l'analisi di secondo livello deve essere effettuata nel più breve tempo possibile dalla conoscenza dell'evento, o comunque entro 72 ore, come previsto dall'art. 33 GDPR.

Il Gruppo Data Breach deve identificare:

- la categoria di violazione:
  - perdita di riservatezza;
  - perdita di integrità;
  - perdita di disponibilità;
- il supporto oggetto della violazione (es. applicativo, banche dati, servizi server farm, dispositivo mobile, computer, documento cartaceo, etc.);
- i dati oggetto della violazione e i relativi trattamenti censiti nel registro dei trattamenti;
- gli interessati;
- il contenimento del danno come di seguito descritto:
  - limitazione o annullamento degli effetti dell'incidente;
  - raccolta delle prove forensi nel caso sia ipotizzato un reato;
  - determinazione delle azioni possibili di ripristino, ed avvio delle stesse;
  - ripristino dei dati, dei sistemi, dell'infrastruttura e delle configurazioni;
  - valutazione dei tempi di ripristino;
  - verifica dei sistemi recuperati;
  - valutazione delle eventuali vulnerabilità collegate con l'incidente;
  - individuazione delle azioni di mitigazione delle vulnerabilità individuate.

Per facilitare la classificazione del rischio per i diritti e le libertà fondamentali delle persone fisiche, la violazione può essere valutata secondo i livelli di rischio riportati da ENISA (The European Union Agency for Cybersecurity).

L'analisi dei Rischi elaborata da ENISA prende in considerazione i seguenti parametri:

- il contesto del trattamento e tipologia di dati;
- la facilità di identificazione dell'individuo sulla base dei dati violati;
- le circostanze della violazione.

In base a tali parametri si calcola un livello di rischio attraverso la seguente formula:

Rischio = (Contesto x Facilità di identificazione) + Circostanze

Il risultato ottenuto permette la seguente catalogazione dei livelli di rischio:

- Basso (<2): gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (Es. tempo trascorso reinserendo informazioni, fastidi, irritazioni, etc.);
- Medio (tra 2 e 3): gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (Es. costi aggiuntivi, rifiuto di accesso ai servizi dell'Azienda, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, etc.);
- Alto (tra 3 e 4): gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (Es. appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, etc.);
- Molto alto (>4): gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Saranno inoltre valutate, come variabili qualitative dell'impatto temuto, le seguenti eventuali condizioni:

- che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- che si tratti di dati relativi a valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- che si tratti di dati di persone fisiche vulnerabili, in particolare minori;
- che il trattamento riguardi una notevole quantità di dati personali;
- che il trattamento riguardi un vasto numero di interessati.

5.7. Notificazione della violazione all'Autorità di controllo

Qualora, dopo l'analisi di secondo livello, risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, non è necessario procedere con la notifica all'Autorità di controllo.

La documentazione prodotta in fase di analisi e corredata dalle relative motivazioni andrà inserita nel registro dei Data Breach ad opera della struttura Affari Generali.

Nei casi in cui sussista un maggiore livello di rischio il Gruppo Data Breach deve valutare le azioni da intraprendere e predispone la notifica all'Autorità di controllo, tramite il modello presente sul sito del Garante, e, ove necessario, la comunicazione agli interessati, verificando e validando la documentazione pervenuta dalle precedenti fasi di lavoro.

La notifica all'Autorità di controllo deve essere effettuata nel caso in cui i rischi per le persone fisiche non siano trascurabili e solo nei seguenti casi:

- l'Azienda è Titolare del/i trattamento/i dei dati coinvolti nella violazione;
- l'Azienda è Responsabile del trattamento con delega alla notifica.

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, va corredata dei motivi del ritardo.

La notifica all'Autorità di controllo deve descrivere, ove possibile:

- la natura della violazione dei dati personali compresi;
- le categorie e il numero approssimativo di interessati in questione;
- le categorie e il numero approssimativo di registrazioni dei dati personali inquestione;
- il nome e i dati di contatto del DPO;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate, o di cui si propone l'adozione da parte dell'Azienda, per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora non sia possibile fornire fin da subito le informazioni, possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Una volta valutata la necessità di effettuare la notifica della violazione dati subita, ARCS, tramite il Gruppo Data Breach, in collaborazione con il DPO, predispone la segnalazione e la invia all'Autorità garante.

Per l'invio della notifica, verrà utilizzata l'apposita procedura telematica resa disponibile dal Garante nel portale del servizi online dell'Autorità: https://servizi.gpdp.it/databreach/s/.

ARCS è tenuto a valutare le circostanze specifiche di ogni effettiva violazione avvenuta. Pertanto, qualora non disponga di tuti gli elementi di dettaglio dell'incidente, è tenuta comunque ad effettuare la notifica della violazione al Garante entro 72 ore, con le informazioni in suo possesso, classificando come preliminare la notifica effettuata. Una volta ricostruito il quadro completo della violazione. ARCS provvederà alla compilazione del medesimo modulo, individuando come integrativa la notifica in essere.

La struttura Affari Generali curerà l'archiviazione della documentazione riguardante la violazione in modo regolare e puntuale, anche durante il suo sviluppo, così da raccogliere le informazioni necessarie e tutti i dettagli rilevanti, tenute a disposizione dell'Autorità Garante.

5.8. Comunicazioni all'Interessato

ARCS, per il tramite del Gruppo Data Breach, in collaborazione con il DPO, deve, inoltre, informare gli interessati dell'evento anomalo, in tutti i casi in cui, a norma degli artt. 33 e 34 GDPR, la violazione presenta gravi rischi per i diritti e le libertà delle persone fisiche (v. allegato C).

La comunicazione deve essere rivolta all'interessato senza ingiustificato ritardo dall'avvenuta conoscenza e valutazione della violazione, attraverso il canale di comunicazione ritenuto più idoneo.

La comunicazione deve essere intellegibile, concisa, trasparente e facilmente accessibile. Deve

essere utilizzato un linguaggio semplice e chiaro adottando, se possibile, la stessa lingua parlata dall'interessato.

La comunicazione di Data Breach all'interessato deve contenere le seguenti informazioni:

- data e ora della violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa;
- la natura della violazione dei dati personali;
- il nome e i dati di contatto del DPO;
- le probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o di cui si propone l'adozione da parte dell'Azienda per porre rimedio alla violazione dei dati personali e anche, se delcaso, per attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenticondizioni:

- sono state messe 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;salvo i casi in cui la violazione della sicurezza ha comportato la distruzione o laperdita dei dati personali degli interessati;
- sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà delle persone fisiche; in tal caso è necessario documentare le misure nel registro e nella comunicazione all'autorità di controllo;
- 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.

L'Azienda deve effettuare la comunicazione nelle casistiche descritte in precedenza e solo per i trattamenti in qualità di Titolare del Trattamento.

Ulteriori istruzioni (es. eventuale delega alla comunicazione) possono essere definite negli atti di nomina a Responsabile del trattamento, *ex* art. 28 GDPR.

5.9. Documentazione della segnalazione

L'Art. 33 del GDPR prescrive l'obbligo di documentare qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.

Nel registro dei Data Breach, la struttura Affari Generali, documenta ogni singolo evento, sia esso falso, irrilevante o rilevante; in quest'ultimi due casi, devono essere indicate nel registro:

- le conseguenze del Data Breach;
- i provvedimenti adottati per porvi rimedio o attenuarne le conseguenze;
- l'eventuale notifica all'autorità di controllo;
- l'eventuale comunicazione all'Interessato.

Nel registro vanno inserite tutte le segnalazioni di violazione pervenute all'Azienda sia come Titolare del trattamento sia come Responsabile del trattamento.

Per quanto riguarda la documentazione delle violazioni, ARCS tiene conto del parere del DPO in

merito alla struttura, all'impostazione e all'amministrazione della documentazione stessa.

5.10. Identificazione delle aree di miglioramento

Il Gruppo Data Breach, con la collaborazione del Gruppo privacy aziendale, adotta le seguenti azioni di miglioramento previste in fase di applicazione della presente procedura:

- analisi dell'evento con figure tecniche-professionali competenti per individuare le vulnerabilità;
- adozione di nuovi sistemi tecnici di prevenzione/protezione e/o di sistemi di controllo/monitoraggio/allarme;
- individuazione di controlli e misure di sicurezza che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
- valutazione su possibilità di copertura assicurativa;
- azioni informative rivolte ai dipendenti;
- revisione delle relazioni con i Fornitori;
- pianificazione dei test periodici per verificare la validità della presente procedura;
- revisione della procedura, se necessario, e di eventuali altri documenticollegati.

5.11. Gestione della segnalazione in qualità di Responsabile

Nei casi in cui l'Azienda agisca come Responsabile del trattamento di dati personali, il Gruppo Data Breach deve comunicare l'incidente di sicurezza riguardante i dati personali al Titolare con le modalità convenute negli atti di nomina/istruzioni ricevute e con la massima tempestività, fornendo tutte le informazioni necessarie e mettendosi a disposizione di quest'ultimo per approfondimenti e contenimento dei danni.

L'Azienda non ha il dovere di notificare all'Autorità Garante quando agisce come Responsabile del trattamento per conto di altro Titolare (senza delega alla notificaal Garante). Spetta infatti al Titolare la valutazione dell'effettiva sussistenza della violazione di dati personali.

Anche la comunicazione verso l'interessato, nei casi in cui l'Azienda agisca in qualità di Responsabile spetta al Titolare.

Quindi, va comunque documentato l'incidente di sicurezza riguardante i dati personali, come descritto al paragrafo 2.4.6. "Documentare la segnalazione".