Gestione delle segnalazioni delle violazioni di dati personali – Data Breach

Atteso che l'art. 33 del Regolamento UE 679/2016 prevede quanto segue: "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" e che l'art. 34 del Regolamento UE 679/2016 prevede quanto segue: "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",

si riporta quanto segue:

1. Ruoli e responsabilità

Coerentemente con il modello organizzativo in ambito Data Protection adottato dalla Struttura, si riportano i ruoli e le responsabilità di ciascuna figura coinvolta nel processo di segnalazione delle violazioni (di seguito, "Data Breach"):

(i) Titolare del Trattamento (Titolare): notifica la violazione all'autorità di controllo competente (Garante) senza ingiustificato ritardo, a meno che sia improbabile che la violazione dei dati presenti un rischio per i diritti e delle libertà delle persone fisiche;

(ii) Referente data breach: coordina le attività dei soggetti autorizzati al trattamento e si interfaccia con gli Amministratori di Sistema; rappresenta il soggetto da informare in caso di incidente che comporti la violazione dei dati personali, informa tempestivamente il Titolare; fornisce, con l'ausilio dei soggetti autorizzati al trattamento e degli Amministratori di Sistema (AdS), elementi utili al Titolare per la predisposizione delle comunicazioni da inviare al Garante privacy e, se necessario, agli interessati;

(iii) Responsabile della protezione dei dati (di seguito anche Data Protection Officer - DPO): funge da punto di contatto tra il titolare, il Garante e interessati. Nell'ambito della gestione degli incidenti, una volta che il Referente data breach abbia accertato la violazione, può supportare su richiesta il Titolare nella predisposizione della notifica che quest'ultimo invierà al Garante privacy e, se necessario, agli interessati. Risponde inoltre ad eventuali richieste di ulteriori informazioni da parte del Garante;

(iv) Soggetti autorizzati al trattamento: soggetti preposti materialmente ad una o più attività di trattamento che coadiuvano il Referente data breach coerentemente con le responsabilità attribuitegli, svolgendo le seguenti attività:

i. comunicano al Referente data breach eventuali violazioni di dati personali mediante gli appositi strumenti e canali;
ii. supportano in fase di identificazione dell'incidente, fornendo al Referente data breach informazioni utili per la classificazione delle violazioni verificatesi;

(v) Amministratori di Sistema (AdS): soggetti che, in qualità di preposti alle attività di gestione e manutenzione dei sistemi informativi aziendali, coadiuvano il Referente data breach, coerentemente con le responsabilità attribuitegli, svolgendo le seguenti attività:

i. monitorano i sistemi di sicurezza;
ii. comunicano, in caso di violazione, tutte le informazioni necessarie alla sua comprensione e le trasmettono al Referente data breach;
iii. monitorano nel continuo le attività necessarie a prevenire eventuali violazioni e/o le attività che rilevino le eventuali non conformità delle misure di sicurezza;
iv. comunicano al Titolare e al Referente data breach eventuali situazioni che possono comportare violazioni di dati personali;
v. raccolgono le informazioni per quanto di competenza necessarie a formulare compiutamente le comunicazioni verso il Garante/Interessato;
vi. attuano, ove possibile, interventi volti a limitare il danno.

1.1.1 Identificazione e definizione delle violazioni di dati personali

Con il termine "violazione dei dati personali" ("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 Ue 679/2016 come dati personali, trasmesse, memorizzate o elaborate per mezzo di sistemi informatici.

Coerentemente con il contenuto di cui al Documento WP 250 – *Guidelines on Personal data breach notification under Regulation 2016/679,* le violazioni possono essere classificate in base ai seguenti principi di sicurezza delle informazioni:

- "violazione della riservatezza", in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- "violazione della disponibilità", in caso di perdita accidentale o non autorizzata di accesso o distruzione di dati personali;
- "violazione dell'integrità", in caso di alterazione non autorizzata o accidentale dei dati personali.

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

- furto o smarrimento di beni aziendali, 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 aziendali, 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 aziendali, ad esempio, mediante l'introduzione di software dannoso, l'inclusione di codice malware ovvero di attacchi di phishing a danno dei dipendenti/collaboratori e al fine di sottrarre i dati ed informazioni di carattere personale;

- 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;

- mancata vigilanza/adozione misure di sicurezza, qualora, causa di un'erronea valutazione sul livello di criticità dei dati e/o informazioni aziendali, non sono state poste in essere le necessarie precauzioni per salvaguardarle.

2. Processo di gestione della segnalazione dei dati personali

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

2.1 Rilevazione della violazione

Gli Amministratori di Sistema e/o i Soggetti autorizzati al trattamento che vengano a conoscenza o sospettano che sia avvenuta una possibile violazione devono darne immediata comunicazione al Referente data breach competente.
Qualora la presunta violazione è avvenuta nei riguardi di dati personali gestiti e/o trattati da un fornitore esterno, nominato Responsabile esterno ai sensi dell'art. 28 del Regolamento UE 679/2016, sarà dovere dello stesso rilevarla e darne comunicazione alla Struttura nella persona del Referente data breach oppure, se quest'ultimo non fosse direttamente contattabile, nella persona del soggetto responsabile della gestione del rapporto con il fornitore. Il responsabile provvederà poi ad avvertire immediatamente il Referente data breach.
Pertanto, indipendentemente dal canale di segnalazione, il processo si attiva con l'avvenuta comunicazione al Referente data breach della presunta violazione da parte degli AdS e/o dei Soggetti autorizzati al trattamento e/o da parte dei soggetti responsabili della gestione dei rapporti con i fornitori esterni.
Le tempistiche previste dalla normativa per la gestione degli adempimenti connessi alle violazioni accertate decorrono dal momento della scoperta della violazione.

2.2 Esecuzione dei riscontri interni

Il Referente data breach, ricevuta la comunicazione della presunta violazione, effettua alcune verifiche interne. In particolare, con l'ausilio degli AdS e dei Soggetti autorizzati al trattamento, esegue i riscontri preliminari e in caso di esito positivo e dunque di accertamento della stessa, comunica tramite e-mail al Titolare e, per conoscenza al DPO, la violazione con specifica indicazione delle seguenti informazioni:

- l'oggetto e la natura della violazione, 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;
- la data e il luogo della violazione;
- una sintetica descrizione dei sistemi informatici utilizzati per la gestione dei dati personali trattati e violati;
- una valutazione di impatto e di gravità della violazione, ivi incluse le probabili conseguenze della violazione dei dati personali;

- una descrizione analitica della violazione;
- le misure adottate o proposte per la risoluzione della violazione intervenuta e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora la violazione sia stata riscontrata dal fornitore esterno, le verifiche del caso saranno poste in essere dal fornitore stesso e le relative risultanze comunicate al Titolare.
Qualora la violazione riscontrata dalla Struttura in qualità di Titolare del Trattamento riguardi trattamenti dei dati gestiti anche da fornitori esterni, tale violazione deve essere segnalata anche ai Responsabile Esterni.

2.3 Analisi della violazione

Il Titolare, se del caso su richiesta con il supporto del DPO, ricevuta la comunicazione della presunta violazione, valuta la complessità della stessa basandosi sulle informazioni ricevute dal Referente data breach o dal fornitore esterno e provvede a registrare la violazione all'interno di un Registro delle Violazioni

La violazione può essere definita complessa utilizzando taluni parametri quali, a mero titolo di esempio, i seguenti:

i. i dati personali sono di carattere sensibile/particolare e/o di natura finanziaria;
ii. il numero di soggetti coinvolti è superiore a n.100;
iii. i sistemi informatici oggetto di violazione sono complessi per qualità/quantità di informazioni elaborate;
iv. 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 (i.e. cifratura), qualora non siano coinvolti interessati, se non in numero limitato e i dati personali siano parziali e non associati ad altre informazioni (i.e. nome e cognome senza codice fiscale o carta di credito o numeri telefonici), la violazione può essere definita non complessa.
Qualora la violazione sia stata riscontrata dal fornitore esterno, gli approfondimenti sulla tipologia di violazione saranno effettuati dal fornitore stesso che comunicherà tramite email gli esiti delle attività svolte al Titolare, dandone evidenza a quest'ultimo in maniera tempestiva, al fine di consentire a quest'ultimo di notificare la violazione al Garante nei termini di legge.

2.4 Comunicazioni al Garante ed esecuzione di ulteriori riscontri (violazione complessa)

Nel caso in cui la violazione avvenuta sia qualificata come complessa, il Titolare predispone una prima comunicazione da inviare al Garante entro le 72h previste per legge dal momento della scoperta della violazione, nella quale sono indicati gli elementi di cui al paragrafo 3.2, oltre al nome e i dati di contatto del DPO.
Successivamente il Titolare, con l'ausilio del Referente data breach, degli AdS e dei Soggetti autorizzati al trattamento e, se del caso su richiesta con il supporto del DPO, esegue ulteriori riscontri necessari a completare le evidenze mancanti rispetto alle prime analisi condotte.
L'esito di tali riscontri è comunicato al Garante tempestivamente e comunque appena possibile in rapporto alla particolare gravità della violazione.
Il Titolare effettua la comunicazione utilizzando il modello di notifica messo a disposizione da parte del Garante sul proprio sito.
I tempi di notifica, nonché l'oggetto delle comunicazioni inviate al Garante, devono essere formalizzate all'interno del Registro delle Violazioni.
Qualora la violazione riscontrata dalla Struttura in qualità di Titolare del Trattamento, riguardi trattamenti dei dati gestiti da fornitori esterni, il Titolare deve comunicare al Responsabile Esterno l'avvenuta comunicazione al Garante effettuata dalla Struttura.
Qualora la violazione sia altresì valutata non complessa verrà trattata come previsto nel paragrafo *3. "Comunicazione al Garante (violazione non complessa)*".

2.5 Comunicazione al Garante (violazione non complessa)

Qualora la violazione di dati personali sia stata valutata non complessa, il Titolare effettua la comunicazione al Garante comunque entro 72h dal momento della scoperta della violazione indicando le informazioni di interesse relative all'evento.
Qualora la violazione riscontrata dalla Struttura in qualità di Titolare del Trattamento, riguardi trattamenti dei dati gestiti da fornitori esterni, il Titolare deve comunicare al Responsabile Esterno l'avvenuta comunicazione al Garante effettuata dalla Struttura.

2.6 Invio comunicazione agli interessati

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare comunica la violazione avvenuta anche agli interessati del trattamento coinvolti, utilizzando i canali ritenuti più appropriati anche in combinazione tra di loro (i.e. SMS, e-mail, pubblicazione su sito web di banner informativi).

2.7 Rivalutazione dei rischi

Una volta concluse le operazioni di comunicazione della violazione, il Titolare effettua una rivalutazione dei rischi che incombono sul trattamento o sui trattamenti che sono stati oggetti di data breach ed identifica e mette in atto le misure necessarie finalizzate ad evitare il ripetersi della violazione o comunque a mitigarne il danno.