PROCEDURA
PER LA RILEVAZIONE
E LA GESTIONE
DI UNA VIOLAZIONE
DEI DATI PERSONALI
(Data Breach)

SCOPO E CAMPO DI APPLICAZIONE

Scopo della presente procedura è quello di descrivere il processo di rilevazione e gestire gli eventuali eventi che potrebbero comportare una violazione dei Dati personali, cosiddetto "Data breach".

Una violazione di Dati personali può avere infatti conseguenze significativamente lesive dei diritti dell'interessato, quali, a titolo esemplificativo, il furto o la frode d'identità, il danno fisico, un danno patrimoniale o reputazionale.

È quindi opportuno disporre di un adeguato sistema di reazione pronto a intervenire secondo schemi predefiniti che contempli le possibili tipologie di violazioni e le misure necessarie ad attenuare gli effetti negativi.

GENERALITA'

Si indicano di seguito a titolo esemplificativo i principali fattori che potrebbero provocare una violazione dei Dati personali e la conseguente necessità di applicare il processo disciplinato dalla Procedura.

1. Fattori di rischio informatico:

- accesso non autorizzato ai sistemi aziendali

possibili minacce: attacchi informatici, abuso di privilegi di accesso;

- compromissione o manomissione fraudolenta dei Dati personali

possibili minacce: transazioni non autorizzate, modifica dei Dati in ambiente di produzione;

- perdita o degrado della qualità dei dati personali

possibili minacce: errori nei processi di alimentazione o trasformazione, inefficiente gestione dei Dati;

- divulgazione impropria o furto di dati informatici personali

possibili minacce: interrogazioni improprie, furto di hardware, smarrimento di hardware, intercettazione delle comunicazioni, utilizzo improprio di software o servizi;

- perdita totale o parziale di Dati personali

possibili minacce: perdita di disponibilità per guasto hardware, perdita di integrità per guasto hardware, errori nel processo di trattamento dei Dati.

2. Fattori di rischio non informatico:

- danni fisici

possibili minacce: incendi, distruzione accidentale di archivi, distruzione intenzionale di archivi;

- eventi naturali

possibili minacce: allagamenti, terremoti;

- divulgazione impropria o furto di dati fisici personali

possibili minacce: furto, copia non autorizzata di archivi fisici.

Ai fini della Procedura, è possibile classificare le violazioni di Dati personali in tre principali tipologie:

- **violazioni della riservatezza**, come nelle ipotesi di divulgazione o accesso accidentale a Dati personali;
- **violazioni comportanti perdita della disponibilità di Dati**, come nei casi di perdita o distruzione (accidentale o non autorizzata);
- **violazione comportanti perdita dell'integrità di Dati**, come nelle ipotesi di alterazione non autorizzata o accidentale. In tale ultimo caso, il processo di gestione del Data Breach si applica ai soli eventi che comportino una compromissione irreversibile, potendosi, nelle altre ipotesi, gestire l'evento nel conteso di un più generico Incidente.

REGOLE e FASI DEL PROCESSO

Le regole e le fasi del processo di rilevazione e gestione di una violazione dei Dati personali che dovranno essere rispettate sono le seguenti:

1. Rilevazione di un potenziale Data Breach, tramite un sistema interno di monitoraggio o dietro a segnalazioni dirette ed indirette provenienti dal personale interno e/o esterno, nonché direttamente dagli interessati;
2. Valutazione preliminare dell'Incidente tramite un'analisi dettagliata del perimetro di informazioni colpito, al fine di verificare la possibilità che si sia verificata effettivamente una violazione dei Dati personali;

3. Identificazione degli elementi del potenziale Data Breach tra cui l'origine, le cause, gli asset coinvolti, nonché, laddove possibile, il numero e la tipologia di interessati colpiti;
4. Attuazione immediata delle azioni necessarie a ridurre il più possibile gli effetti dell'eventuale violazione, con la conseguente registrazione della stessa;

5a. Se, all'esito delle valutazioni condotte, il Titolare del Trattamento ritiene che la violazione non comporti rischi per i diritti e le libertà delle persone fisiche, non è necessario provvedere alla la notifica al Garante. In tal caso il Titolare documenta e motiva la decisione assunta.

5b. Se, all'esito delle valutazioni condotte, il Titolare del Trattamento ritiene invece che la violazione comporti rischi per i diritti e le libertà delle persone fisiche – previa definizione della strategia necessaria al fine di minimizzare ogni ulteriore conseguenza ed evitare un peggioramento della situazione – il Titolare invia al Garante, senza ingiustificato ritardo, e comunque **entro 72 ore dal momento in cui è venuto a conoscenza della violazione**, apposita notifica.

1. Se, all'esito delle valutazioni condotte, il Titolare del Trattamento ritiene che la violazione è suscettibile di arrecare un rischio elevato per i diritti e le libertà delle persone fisiche, è necessario provvedere ad informare della violazione gli interessati

Ai sensi dell'art. 33, comma 3 del GDPR, la notifica del Data Breach al Garante deve contenere, almeno, le seguenti indicazioni:

- la descrizione della 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;
- il nome e i dati di contatto del Titolare del Trattamento e del DPO ove previsto;
- le probabili conseguenze della violazione dei Dati personali;

- le misure adottate o di cui si propone l’adozione da parte del Titolare per porre rimedio alla violazione dei Dati personali e per attenuarne ulteriori possibili effetti negativi.

In caso tali regole dovessero essere disattese o non rispettate in tutto o in parte, i soggetti ritenuti responsabili di tali violazioni saranno oggetto di provvedimenti disciplinari.