PROCEDURA INTERNA DI GESTIONE DEL DATA BREACH

Linee guida operative per il rilevamento, la valutazione e la notifica delle violazioni di dati personali (Artt. 33 e 34 del Regolamento UE 2016/679 - GDPR)

PREAMBOLO E FINALITÀ

Ai sensi degli articoli 33 e 34 del GDPR, una violazione dei dati personali (**Data Breach**) consiste in un incidente di sicurezza che comporta, in modo accidentale o illecito, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

In ossequio al principio di **Accountability (Responsabilizzazione)**, la presente procedura definisce le azioni reattive e organizzative repentine che l'intera struttura aziendale deve intraprendere al fine di minimizzare l'impatto dell'incidente, determinare la gravità del rischio per i diritti e le libertà delle persone fisiche, e adempiere agli obblighi di legge nei tempi tassativi previsti dalla norma.

1. CLASSIFICAZIONE DELLE VIOLAZIONI (TIPOLOGIE DI RISCHIO)

Una violazione di sicurezza può classificarsi in tre macro-categorie, le quali possono presentarsi anche congiuntamente:

- **Violazione di Riservatezza:** Divulgazione di dati personali o accesso agli stessi da parte di soggetti non autorizzati (es. phishing riuscito, smarrimento di un PC non cifrato, e-mail massive inviate in chiaro invece che in copia conoscenza nascosta).
- **Violazione di Integrità:** Alterazione non autorizzata o accidentale dei dati personali originari che ne comprometta l'esattezza o l'affidabilità (es. manomissione di un database).
- **Violazione di Disponibilità:** Perdita dell'accesso o distruzione accidentale o illecita dei dati personali (es. attacco Ransomware che cifra i server aziendali, incendio di un archivio cartaceo privo di copie digitali).

2. FLUSSO DI GESTIONE DELL'INCIDENTE (FASI OPERATIVE)

Fase 2.1: Rilevamento e Segnalazione Interna

Qualunque dipendente, collaboratore o amministratore di sistema che identifichi o sospetti un'anomalia di sicurezza ha l'**obbligo tassativo di segnalare immediatamente** l'evento via e-mail al punto di riferimento interno e ai canali di riferimento dello Studio. L'operatore non deve tentare di risolvere l'anomalia in autonomia o occultarla.

Fase 2.2: Contenimento Immediato e Mitigazione

Il reparto IT o i fornitori di servizi informatici esterni (Responsabili ex art. 28) attivano d'urgenza le prime misure di contenimento volte a circoscrivere la falla. Esempi d'azione includono: isolamento dei server infetti dalla rete

locale aziendale, revoca o reset delle credenziali compromesse, interruzione momentanea di specifici flussi web o canali di trasmissione.

Fase 2.3: Analisi del Rischio e Valutazione della Gravità

Il Titolare del Trattamento, con il supporto e il parere vincolante del **Data Protection Officer (DPO)**, procede a valutare l'evento sulla base dei seguenti parametri oggettivi:

- Natura, volume e categorie di dati coinvolti (con particolare focus sulla presenza di dati sensibili/giudiziari).
- Numero approssimativo di interessati coinvolti.
- Presenza di adeguate misure di protezione tecniche preventive (es. se i file sottratti erano protetti da crittografia forte e robusta, il rischio di decifrazione da parte di terzi è da considerarsi nullo).

3. ADEMPIMENTI DI LEGGE E TEMPISTICHE TASSATIVE

Dall'esito dell'analisi del rischio si configurano tre scenari normativi distinti:

SCENARIO A: RISCHIO ASSENTE O IMPROBABILE

Se la violazione è ritenuta improbabile che presenti un rischio per i diritti delle persone fisiche, il Titolare non effettua notifiche esterne. L'evento viene esclusivamente documentato e descritto all'interno del **Registro interno dei Data Breach** aziendale.

SCENARIO B: PRESENZA DI RISCHIO → NOTIFICA AL GARANTE ENTRO 72 ORE

Qualora l'incidente presenti un rischio concreto per gli interessati, il Titolare deve notificare la violazione all'Autorità Garante per la Protezione dei Dati Personali **entro il termine perentorio di 72 ore** dal momento in cui ne è venuto a conoscenza (art. 33 GDPR). Le notifiche tardive devono essere accompagnate da una motivazione documentata del ritardo.

SCENARIO C: PRESENZA DI RISCHIO ELEVATO → COMUNICAZIONE AGLI INTERESSATI

Se l'impatto della violazione comporta un rischio *elevato* (es. furto di credenziali bancarie, dati sanitari o furto d'identità), il Titolare ha l'obbligo di comunicare l'avvenuto incidente **tempestivamente e direttamente a tutti gli interessati** coinvolti (art. 34 GDPR), indicando con chiarezza la natura della violazione e i suggerimenti per autotutelarsi (es. cambiare le password in uso).

4. IL REGISTRO DEI DATA BREACH

Tutte le violazioni di sicurezza, comprese quelle non soggette all'obbligo di notifica al Garante, devono essere fedelmente inserite nel **Registro delle Violazioni**. Il registro deve contenere:

- Descrizione dettagliata del fatto, delle cause e del contesto dell'incidente.
- Le categorie e il numero di interessati e record di dati personali coinvolti.

- Le conseguenze reali o potenziali derivanti dall'evento.
- Le misure di mitigazione adottate nell'immediato e quelle strutturali pianificate per impedire il ripetersi della falla.

Questo registro rappresenta il primo documento ispezionato dalle Autorità in caso di verifiche o audit di conformità aziendale.