PROCEDURA DI GESTIONE DEL DATA BREACH
AI SENSI DEGLI ARTT. 33 E SS REGOLAMENTO (UE) 2016/679

Premessa:

Per data breach deve intendersi la violazione dei dati personali che ricorre quando una delle misure tecnico-organizzative adottate dal titolare del trattamento, pur reputate adeguate, non ha retto e si è rivelata inidonea a fronteggiare il rischio per la protezione dei dati personali, per la libertà, i diritti, i legittimi interessi degli interessati.

Cosa deve fare il titolare in caso di data breach:

1) Ai sensi dell'art. 33 GDPR, **il titolare del trattamento notifica la violazione all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore** dal momento in cui ne è venuto a conoscenza.

2) Il titolare omette la notifica se ritiene improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone.

3) Nel caso di mancato rispetto del termine di 72 ore, il titolare corredata la notifica della violazione delle ragioni del ritardo.

4) La notifica contiene:

- descrizione della natura della violazione dei dati personali con indicazione di:

    ⇒ data presunta e luogo di verificazione dell'evento anomalo / dell'avvenuta violazione

    ⇒ data e ora in cui si è avuto conoscenza della violazione

    ⇒ fonte da cui si è appresa l'avvenuta violazione (per es. segnalazione dell'interessato)

    ⇒ tipologia di violazione ed informazioni coinvolte (per es. accesso abusivo al sistema gestionale con apprensione illegittima dell'anagrafica clienti)

    ⇒ numero di interessati coinvolti e dei dati personali di cui si presume la violazione (nell'esempio sopra, numero dei clienti e dei relativi dati)

    ⇒ categorie di dati di cui si presumere la violazione, con particolare riguardo a dati sensibili e dati relativi a minori (nell'esempio sopra, dati anagrafici dei clienti, dati inerenti al loro stato di salute);

- nome e dati di contatto del referente presso cui è possibile ottenere maggiori informazioni o del responsabile della protezione dei dati (RPD) eventualmente nominato;

- descrizione delle probabili conseguenze della violazione dei dati personali, a titolo esemplificativo e non esaustivo:

    ⇒ discriminazioni

⇒ furto o usurpazione d'identità

⇒ perdite finanziarie, danno economico, altri danni per le persone fisiche coinvolte

⇒ pregiudizio alla reputazione

⇒ perdita di riservatezza dei dati personali protetti da segreto professionale

⇒ privazione o limitazione di diritti o libertà;

- descrizione delle misure adottate dal titolare o da adottare per porre rimedio alla violazione dei dati personali e/o per attenuarne le conseguenze negative, a titolo esemplificativo e non esaustivo:

⇒ tempestiva denuncia alle autorità anche al fine di rintracciare il responsabile

⇒ ripristino dei dati conservati attraverso i meccanismi di back up, di cyber resilience, di continuità operativa utilizzati dal titolare

⇒ modifica di chiavi di accesso fisiche e logiche ai dati.

Se non è possibile fornire le informazioni contestualmente alla notifica, il titolare le fornisce successivamente ma, comunque, senza ulteriore ingiustificato ritardo.

5) Della violazione dei dati personali è conservata traccia da parte del titolare, mediante la predisposizione di idonea documentazione che indichi le circostanze in cui la violazione si è verificata, le relative conseguenze, nonché le misure adottate per porvi rimedio. La documentazione della violazione permette, tra l'altro all'autorità di controllo di verificare il rispetto della procedura di notifica di cui al citato art. 33 GDPR.

6) Ai sensi dell'art. 34 GDPR, **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.**

7) La comunicazione, formulata con un linguaggio semplice e chiaro, indica almeno:

- nome e dati di contatto del referente presso cui è possibile ottenere maggiori informazioni o del responsabile della protezione dei dati (RPD) eventualmente nominato;

- descrizione delle probabili conseguenze della violazione dei dati personali;

- descrizione delle misure adottate dal titolare o da adottare per porre rimedio alla violazione dei dati personali e/o per attenuarne le conseguenze negative.

8) L'obbligo di comunicazione della violazione all'interessato viene meno se:

- il titolare ha adottato misure tecnico - organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione (in particolare misure di pseudominizzazione e cifratura)

- il titolare ha successivamente adottato misure volte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

- la comunicazione della violazione richiederebbe sforzi sproporzionati: in tal caso, il titolare effettua una comunicazione pubblica tramite la quale gli interessati sono informati con analoga efficacia.

9) L’autorità di controllo può richiedere al titolare di effettuare la comunicazione all’interessato, qualora non vi abbia ancora provveduto e sussista la probabilità che la violazione dei dati personali presenti un rischio elevato.

10) Nell’atto di nomina a responsabile del trattamento, il titolare impartisce al responsabile l’obbligo di segnalare immediatamente per iscritto qualunque evento, elemento, fatto che possa essere rilevante in termini di sicurezza dei dati personali trattati, dei diritti e della libertà degli interessati, ai fini di garantire il tempestivo intervento in caso di violazione dei dati.

11) Nell’atto di nomina a incaricato del trattamento, il titolare impartisce all’incaricato l’obbligo di segnalare immediatamente ogni comportamento e ogni fatto atto ad integrare una violazione dei dati personali, nonché ogni malfunzionamento dei sistemi informatici in uso. L’incaricato deve comunicare, in particolare, la data di rilevazione del rischio, la localizzazione del rischio, la descrizione del rischio e ogni altra informazione utile a prevenire un illecito trattamento, una violazione dei dati personali, nonché a limitarne le conseguenze dannose.