Procedura “Gestione delle Violazioni di Dati Personali” – Allegato 1
Tipologia di violazione

Tipologia di violazione

Una Violazione dei dati personali è 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:

- «Distruzione»: i dati non esistono più o non esistono più in una forma che sia di qualche utilità per il Titolare del trattamento.
- «Alterazione»: i dati sono stati modificati, corrotti o non sono più completi.
- «Perdita»: i dati potrebbero comunque esistere, ma il Titolare ne ha perso il controllo o l’accesso, oppure non ne è più in possesso. Esempi:
    - un dispositivo contenente una copia della banca dati dei clienti del titolare è stato perso o rubato
    - l’unica copia di un insieme di dati personali sia stata cifrato da un ransomware oppure dal titolare mediante una chiave non più in suo possesso.
- «Divulgazione o accesso non autorizzati»: i dati sono stati rivelati/trasmessi o acceduti da destinatari non autorizzati

I Data Breach possono essere categorizzati secondo i seguenti ben noti principi di sicurezza delle informazioni:

- “Perdita di riservatezza”, dove si verifica una rivelazione o accesso non autorizzato o accidentale a dati personali;
- “Perdita di integrità”, dove si verifica un’alterazione non autorizzato o accidentale dei dati personali
- “Perdita di disponibilità”, dove si verifica perdita d’accesso o una distruzione non autorizzato o accidentale dei dati personali;

Si ha una perdita di disponibilità quando:

- i dati sono stati cancellati accidentalmente oppure intenzionalmente (da un soggetto non autorizzato) o, nel caso di dati cifrati, la chiave di decifratura è stata persa. Se il titolare non è in grado di ripristinare l’accesso ai dati per esempio da un backup, si tratta di una perdita di disponibilità permanente;
- si verifica una significativa interruzione del normale servizio di un’organizzazione, per esempio a causa di un attacco di *“denial of service”* che renda i dati indisponibili.
- si verifica una significativa interruzione di servizio dovuta ad un guasto, quindi in assenza di meccanismi di garanzia della continuità del servizio.

Nel caso di perdita di disponibilità temporanea, la necessità di notificare o meno all’Autorità una Violazione dipende dai casi. Ad esempio, in un ospedale, se dati sanitari critici sui pazienti non sono disponibili, anche temporaneamente, ciò potrebbe rappresentare un rischio per i diritti e le libertà individuali: interventi potrebbero dover essere cancellati e vite umane a rischio. Diversamente, se una media company non è in grado di inviare newsletter a causa di un blackout che rende il suo sistema informatico indisponibile per diverse ore, è improbabile che ciò presenti un rischio per i diritti e le libertà

Un data breach può incidere singolarmente su riservatezza, disponibilità ed integrità oppure anche contemporaneamente su più di una di esse o consistere anche in una combinazione delle suddette violazioni.

Ad esempio, nel caso di perdita del supporto fisico di memorizzazione dei dati (es. furto o smarrimento dei dispositivi contenti i dati oppure dei documenti cartacei), si verifica solo una perdita di riservatezza laddove non si tratta dell’unica copia dei dati. Nel caso (raro) in cui i dati non possano essere recuperati da un back up si tratterebbe anche di una perdita di disponibilità.