# SCHEMA DI VALUTAZIONE VIOLAZIONI/DATA BREACH

## ESEMPI

| TIPO DI DATA BREACH | DEFINIZIONE | SEGNALAZIONE AL GARANTE NECESSARIA | ESEMPI DI SEGNALAZIONE | CONTROESEMPI (SEGNALAZIONE NON NECESSARIA) |
|---|---|---|---|---|
| **Distruzione** | Un insieme di dati personali, a seguito di un incidente o azione fraudolenta, non è più nella disponibilità del Titolare, né di altri. In caso di richiesta del dato da parte dell'interessato, non è possibile produrlo. | I dati non sono più recuperabili o provenienti da procedure o processi non ripetibili e che non possono, quindi, essere ulteriormente generati. | • Guasto non riparabile dell'hard disk contenente uno o più documenti che, in violazione del regolamento, erano stati salvati localmente.<br>• Incendio di archivio cartaceo. | • Rottura di una chiavetta USB che non contiene dati personali originali<br>• Rottura di un PC che non contiene dati personali originali<br>• Distruzione di un documento, ad esempio a causa di un guasto di sistema |
| **Perdita** | Un insieme di dati personali, a seguito di un incidente o azione fraudolenta, non è più nella disponibilità del Titolare, ma potrebbe essere nella disponibilità di terzi (in maniera lecita o illecita). In caso di richiesta del dato da parte | Dati non recuperabili o provenienti da procedure o processi non ripetibili e che non possono, quindi, essere ulteriormente generati<br>Dati la cui indisponibilità lede i diritti fondamentali dell'interessato<br>Dati per i quali la | • Smarrimento di chiavetta USB contenente dati personali<br>• Smarrimento di fascicolo cartaceo personale dipendente | • Smarrimento di un documento, ad esempio a causa di un guasto di sistema |

| | | | | |
|---|---|---|---|---|
| | dell'interessato non è possibile produrlo, mentre è possibile che terzi ne possano avere impropriamente accesso | divulgazione, conseguente alla perdita, possa ledere i diritti fondamentali dell'interessato | | |
| **Modifica** | Un insieme di dati personali, a seguito di un incidente o azione fraudolenta, è stato irreversibilmente modificato, senza la possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non è possibile produrlo con la certezza che non sia stato alterato. | Dati per i quali non è possibile avere certezze sulla consistenza e sull'assenza di alterazioni | • Guasto tecnico che altera parte dei contenuti di un sistema, compromettendo anche ibackup<br>• Azione involontaria o fraudolenta che porta all'alterazione di dati in modo non tracciato e irreversibile | • Guasto tecnico che altera parte dei contenuti di un sistema, rilevato e sanato tramite operazioni di *Disaster Recovery*<br>• Azione involontaria di un utente che porta all'alterazione di dati tracciata e reversibile<br>• Modifica di un documento non ancora validato dal proprio autore |
| **Divulgazione non autorizzata** | Un insieme di dati personali (e riconducibili all'individuo in maniera diretta o indiretta), a seguito di un incidente o azione fraudolenta, è stato trasmesso a terze parti senza il consenso dell'interessato | Dati per i quali la divulgazione, conseguente alla perdita, possa ledere i diritti fondamentali dell'interessato | • Consegna di un CD con dati ad altra struttura senza autorizzazione | • Infezione virale di un PC con un virus che dalla scheda tecnica non trasmette dati all'esterno dell'organizzazione |

| | | | | |
|---|---|---|---|---|
| **Accesso non autorizzato** | Un insieme di dati personali (e riconducibili all'individuo in maniera diretta o indiretta), sono stati resi disponibili per un intervallo di tempo a persone non titolate ad accedere al dato | Dati per i quali la divulgazione, conseguente alla perdita, possa ledere i diritti fondamentali dell'interessato | • Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi<br>• Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema | • Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi |
| **Indisponibilità temporanea** | Un insieme di dati personali, a seguito di un incidente o azione fraudolenta o involontaria, non è più disponibile per un periodo di tempo che lede i diritti dell'interessato | Dati per i quali l'indisponibilità eccede possa ledere i diritti fondamentali dell'interessato | • Infezione da ransomware che comporta la temporanea perdita di disponibilità dei dati e questi non possono esser ripristinati dal backup | • Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso |

## STRUMENTO DI AUTOVALUTAZIONE GARANTE PRIVACY

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante Privacy ha ideato e messo disposizione un apposito **strumento di autovalutazione (self assessment)** che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

| N. | Tema/requisito | Sì | No | N.A. | Note |
|---|---|---|---|---|---|
| 1 | C'è stato un *data breach*, come è opportuno procedere? | ☐ | ☐ | ☐ | Ai sensi dell'articolo 4 GDPR, la violazione di dati personali consiste in 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. Il Titolare valuta se l'incidente rientra nella definizione di violazione di dati personali. |
| 2 | In caso di violazione, è opportuno raccogliere tutte le relative informazioni.<br>1. Quali dati personali sono coinvolti nell'incidente di sicurezza?<br>2. A quale categoria di Interessati appartengono?<br>3. Quanti Interessati sono stati coinvolti?<br>4. Quando si è verificato l'incidente? | ☐ | ☐ | ☐ | Il Titolare del trattamento deve notificare l'eventuale *data breach* all'Autorità di controllo senza ingiustificato ritardo ed entro 72 ore da quando ha avuto conoscenza della violazione. |
| 3 | Quali soggetti sono coinvolti nell'incidente? Una funzione interna? Un fornitore? Un'altra società del gruppo? | ☐ | ☐ | ☐ | |
| 4 | È stata avviata una procedura di *incident response plan* (piano di risposta agli incidenti)? | ☐ | ☐ | ☐ | La procedura di gestione dei *data breach* deve contenere le diverse azioni da implementare per gestire la violazione<br>– internamente e<br>– nei confronti dei fornitori, qualora la violazione sia avvenuta nell'ambito dei servizi affidati ad un fornitore esterno. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Sono inoltre indicate le responsabilità di ciascun membro del team addetto alla gestione delle violazioni. |
| 4 (a) | [In relazione alla domanda 4] In caso di Responsabili del trattamento, è stata data immediata comunicazione al Titolare e documentato quanto accaduto, oltre che la relativa comunicazione al Titolare? | ☐ | ☐ | ☐ | Il Titolare del trattamento deve documentare qualsiasi violazione, le relative circostanze, le conseguenze e i provvedimenti adottati per porre rimedio. Per tale ragione il Responsabile è tenuto a trasmettere ogni informazione al Titolare e collaborare con quest'ultimo per la gestione del *data breach* e l'adozione di misure di rimedio. |
| 5 | Quale tipo di *data breach* è intervenuto? | ☐ | ☐ | ☐ | Ai sensi dell'articolo 4 del GDPR, la violazione di dati personali può consistere<br>– nella distruzione,<br>– la perdita,<br>– la modifica,<br>– la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o trattati. |
| 6 | Sono stati valutati i rischi per le libertà e i diritti delle persone fisiche? | ☐ | ☐ | ☐ | |
| 6 (a) | [In relazione alla domanda 6] Non sussistono rischi per le libertà e i diritti delle persone fisiche. Non è pertanto prevista la notifica all'Autorità di controllo e il questionario si conclude qui. | ☐ | ☐ | ☐ | **È necessario in ogni caso**<br>1. documentare internamente la violazione dei dati personali nell'apposito registro e<br>2. valutare le azioni di rimedio e di mitigazione per evitare un incidente simile in futuro.<br>Se il Titolare ha stabilito di non notificare la violazione **dovrà documentare** tale decisione e la relativa giustificazione. |

| | | | | | |
|---|---|---|---|---|---|
| 6 (b) | [In relazione alla domanda 6] Sussistono rischi per le libertà e i diritti delle persone fisiche, è prevista la notifica all'Autorità di controllo. Procedere con il questionario. | ☐ | ☐ | ☐ | Ai sensi dell'articolo 33 GDPR, <u>la notifica deve contenere</u> **<u>almeno</u>**:<br>- la descrizione della natura della violazione, compreso, ove possibile, le categorie e il numero di Interessati coinvolti nonché le categorie e il numero di registrazioni dei dati personali<br>- Il nome e i dati di contatto del Responsabile della protezione dei dati o altro contatto presso cui ottenere le informazioni<br>- la descrizione delle probabili conseguenze delle violazioni dei dati personali<br>– la descrizione delle misure adottate o di cui è prevista l'adozione per porre rimedio alla violazione e per attenuare i possibili effetti negativi |
| 7 | [In relazione alla domanda 6] | ☐ | ☐ | ☐ | I rischi per le libertà e i diritti delle persone fisiche **sono elevati**? Nel **valutare i rischi** è importante focalizzare <u>l'attenzione sulle possibili conseguenze negative per gli individui</u>. Una violazione di dati personali può anche provocare *danni fisici, materiali o immateriali ai soggetti interessati,* ad *esempio*<br>– discriminazione,<br>– furto o usurpazione di identità,<br>– perdite finanziarie,<br>– decifratura non autorizzata della pseudonimizzazione,<br>– pregiudizio alla reputazione,<br>– perdita di riservatezza dei dati personali protetti da segreto professionale,<br>– etc.<br>(Considerando 85). |
| 7 (a) | [Relativamente alla domanda 7] Se la risposta è negativa, e i rischi non sono elevati, non si procede con la notifica agli Interessati e il questionario si conclude qui. | ☐ | ☐ | ☐ | **È necessario in ogni caso**<br>– documentare internamente la violazione dei dati personali nell'apposito registro |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | – e valutare le azioni di rimedio e di mitigazione per evitare un incidente simile in futuro. |
| 7 (b) | [Relativamente alla domanda 7] Se la risposta è affermativa, il rischio è elevato, procedere con il questionario e valutare se nonostante il rischio elevato si sia in presenza delle eccezioni di cui all'articolo 34 GDPR. | ☐ | ☐ | ☐ | |
| 8 | [In relazione alla domanda 7] Sono state implementate delle ***misure tecniche e organizzative adeguate*** per la protezione dei dati personali oggetto della violazione? Ad esempio la *cifratura dei dati* o la *pseudonimizzazione*? | ☐ | ☐ | ☐ | |
| 8 (a) | [In relazione alla domanda 8] Se la risposta è negativa, procedere con la comunicazione agli Interessati. | ☐ | ☐ | ☐ | Ai sensi dell'articolo 34 GDPR la comunicazione agli Interessati descrive con un linguaggio semplice e chiaro la natura della violazione e contiene almeno le seguenti informazioni:<br>- il nome e i dati di contatto e i dati di contatto del Responsabile della protezione dei dati o altro contatto presso cui ottenere le informazioni;<br>- la descrizione delle probabili conseguenze delle violazioni dei dati personali;<br>- la descrizione delle misure adottate o di cui è prevista l'adozione per porre rimedio alla violazione e per attenuare i possibili effetti negativi. |
| 8 (b) | [In relazione alla domanda 8] se la risposta è affermativa, non si procede con la comunicazione agli interessati. | ☐ | ☐ | ☐ | **È necessario in ogni caso**<br>– documentare internamente la violazione dei dati personali nell'apposito registro<br>– e valutare le azioni di rimedio e di mitigazione per evitare un incidente simile in futuro. |
| 9 | [In relazione alla domanda 7] Sono state adottate | ☐ | ☐ | ☐ | Tale azione se implementata rientra nelle **eccezioni di cui all'articolo 34** |

| | | | | | |
|---|---|---|---|---|---|
| | **successivamente** alla violazione ***misure volte a prevenire un rischio elevato per i diritti e le libertà delle persone fisiche***? | | | | GDPR, per il quale non è richiesta la comunicazione all'Interessato. |
| 9 (a) | [In relazione alla domanda 9] Se la risposta è negativa, procedere con la comunicazione agli Interessati | ☐ | ☐ | ☐ | |
| 9 (b) | [In relazione alla domanda 9] Se la risposta è affermativa, non si procede con la comunicazione agli Interessati. | ☐ | ☐ | ☐ | **È necessario in ogni caso**<br>– documentare internamente la violazione dei dati personali nell'apposito registro<br>– e valutare le azioni di rimedio e di mitigazione per evitare un incidente simile in futuro. |
| 10 | [In relazione alla domanda 7] La comunicazione agli Interessati richiede uno **sforzo sproporzionato**? | ☐ | ☐ | ☐ | Tale valutazione è opportuna al fine di valutare se sia possibile procedere con una comunicazione pubblica agli Interessati [articolo 34 (3) (c) GDPR] |
| 10 (a) | [In relazione alla domanda 10] Se la risposta è negativa, procedere con la comunicazione agli Interessati | ☐ | ☐ | ☐ | |
| 10 (b) | [In relazione alla domanda 10] Se la risposta è affermativa procedere a una **comunicazione pubblica** agli Interessati. | ☐ | ☐ | ☐ | Tramite la **comunicazione pubblica**, gli Interessati devono essere informati *con analoga efficacia* rispetto alla comunicazione singola. |