Documento	REGISTRO VIOLAZIONI INFORMATICHE
Classe / tipologia	Registro / Politiche della Sicurezza privacy e PD
Adempimenti	PROVV. "**DATA BREACH**" 2/7/2015 - Artt. **32 e 33 REG.679/16**
Documenti relati	INDEX679, SOP3_3, DT679, **RV-DB01**, DVR/IP, **DP-PG679**
Basi giuridiche	Piano di adeguamento 2025-26

CONTENUTI

- Istruzione operativa del Sistema di Controllo e monitoraggio Data Breach
- **ISTRUZIONE E FORMAZIONE PER "LA DATA BREACH" IN AZIENDA**

Questo documento fa compendio con la procedura di gestione **DB-PD679** e la Procedura Operativa in essa contenuta **PROII**. Taki riferimenti, congiuntamente considerati, rappresentano la struttura e le prassi funzionali del sistema aziendale approntato per adempiere agli obblighi del c.d. provvedimento di "Notifica della violazione dei dati" o la c.d. "*Data Breach*".

Il contenuto seguente riporta la politica delle pratiche adottate sulle quali è stata svolta adeguata formazione e affiancamento (Vedi Piano di Formazione, **PDFA**).

SOMMARIO PROCEDURE PASSO PASSO

1. AVVISARE SENZA INDUGIO LE PERSONE COMPETENTI
2. QUALIFICARE E QUANTIFICARE LA VIOLAZIONE
3. ADOTTARE LE MISURE NECESSARIE PER MINIMIZZARE LE CONSEGUENZE
4. EFFETTUARE LE NOTIFICAZIONI ALL'AUTORITÀ GARANTE, A MENO CHE NON SIA IMPROBABILE CHE SUSSISTA UN RISCHIO PER I DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE
5. SE IL RISCHIO È ELEVATO EFFETTUARE LE COMUNICAZIONI ANCHE AGLI INTERESSATI
6. IN OGNI CASO ANNOTARE TUTTE LE VIOLAZIONI (ANCHE SE NON NOTIFICATE) NEL REGISTRO DELLE VIOLAZIONI (**RV-DB01**)

A compendio dello schema procedurale si veda la videografica della Autorità di Controllo in allegato al MSPPD "**RG-DB Garante.PDF"**

☐ TITOLARE .....

☐ RESPONSABILE .....

☐ TEAM DI LAVORO .....

☐ ADS / DBA .....

ISTRUZIONE E FORMAZIONE PER LA "DATA BREACH" IN AZIENDA

In virtù degli **Artt. 33 e 34 del GDPR** il Titolare del Trattamento (TDT) deve notificare tutte le violazioni dei dati personali al Garante e comunicare con le Persone Interessate in caso di alto rischio per i diritti e la libertà personali.

La violazione dei dati personali, il c.d. ***data breach***, è una violazione della sicurezza che comporta accidentalmente o illecitamente, distruzione, perdita, alterazione, divulgazione o accesso non autorizzati di dati di natura personale trasmessi, conservati o altrimenti elaborati.

Il titolare del trattamento ha l'obbligo di documentare - e di esibire ad eventuale richiesta del Garante - qualsiasi violazione dei dati personali, le circostanze che l'hanno causata, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Se il Titolare si è avvale di un Responsabile del Trattamento (o Referente Privacy), quest'ultimo ha l'obbligo di notificare al Titolare, senza ingiustificato ritardo dal momento in cui ne viene a conoscenza, qualsiasi violazione dei dati personali. È raccomandabile che tale obbligo sia oggetto di una specifica clausola contrattuale con il RDT e questo deve avvalersi del supporto di un Gruppo di Risposta agli Incidenti Informatici (**GDR-II** come da nomine e designazioni).

In caso di alta probabilità di rischio dei diritti e delle libertà personali, il TDT deve notificare al Garante e comunicare agli interessati tutte le violazioni dei dati personali di cui viene a conoscenza.

In applicazione del principio generale di *Accountability* (**Art. 29**), è rimessa al Titolare del Trattamento la valutazione di probabilità o meno che lo specifico *data breach* possa presentare un rischio per i diritti e le libertà degli assistiti e degli interessati. Laddove la valutazione abbia esito affermativo, non oltre le **72 ore** dalla presa di coscienza (**GDPR, Art. 33**) il TDT deve notificare la violazione al Garante della protezione dei dati personali (in qualità di autorità competente), specificando, tra l'altro:

- ***la natura della violazione dei dati personali (categorie e numero approssimativo di persone e record di dati in questione);***
- ***Il nome e le informazioni di contatto del DPO (se applicabile) o, comunque, di un punto di contatto da cui è possibile ottenere ulteriori informazioni;***
- ***le implicazioni di rischio e conseguenze della violazione;***
- ***le misure adottate o da adottare per mitigare qualsiasi conseguenze negative.***

Il modulo per la notifica – solo online – della violazione dei dati personali è a disposizione del Titolare sul sito del Garante (vedi **PG-DB01**).

E' peraltro raccomandabile di:

- ***mettere in atto misure per analizzare i rischi del trattamento istituito per i diritti e le libertà delle persone fisiche;***
- ***assicurarsi che le violazioni siano notificate entro 72 ore, in caso contrario spiegare accuratamente le motivazioni del ritardo all'autorità garante;***
- ***indicare nella notifica i fatti della violazione, la natura della violazione, i suoi effetti e le misure adottate per porvi rimedio;***
- ***fare ogni sforzo per documentare il più possibile qualsiasi violazione per consentire all'autorità di vigilanza di verificare la conformità ai requisiti imposti dal GDPR;***
- ***mettere immediatamente in atto misure di emergenza per porre rimedio alla violazione e mitigare le conseguenze.***

Comunicazione alle persone interessate

Laddove il titolare valuti che sia probabile che la violazione sia suscettibile di presentare un elevato rischio per i diritti e le libertà di una persona fisica, sarà necessario comunicare anche all'interessato il data breach. Tale comunicazione deve contenere almeno:

- ***le informazioni del nome e dei dati di contatto del DPO (se applicabile) o di altro punto di contatto presso cui ottenere maggiori informazioni;***
- ***la descrizione semplice e chiara della natura della violazione dei dati personali e delle probabili conseguenze, le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.***

La comunicazione all'interessato può non essere necessaria se:

- ***le misure tecniche e organizzative preventivamente approntate dal titolare abbiano hanno reso i dati incomprensibili per qualsiasi persona; ciò capita, ad esempio, quando tali dati, pur diffusi, sono stati cifrati o crittografati;***
- ***sono state adottate misure per garantire che il rischio sia scongiurato e non possa più verificarsi***
- ***la comunicazione richieda "sforzi sproporzionati", ma in questo caso è autorizzata una comunicazione "pubblica" piuttosto che diretta sempreché la stessa possa raggiungere ed informare gli interessati con analoga efficacia della comunicazione diretta.***

Nota: La comunicazione gli interessati può anche essere richiesta dall'Autorità garante se quest'ultima reputa, dopo aver esaminato la notificazione, che vi sia un alto rischio per gli interessati derivante dal data breach.