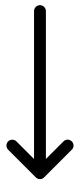
Adempimenti in materia di protezione dei dati personali in seguito ad un *data breach*

A.A. 2022/23

(di Simone Calzolaio)

Cosa è un data breach

Art. 4, par. 12, GDPR: «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».



Quanto accaduto nella organizzazione, ente, azienda, ecc. è un data breach?

Cosa fare per affrontare un data breach

Il titolare che ha già provveduto ad adeguarsi al GDPR (a partire dal 25.5.2018) dovrebbe essere in possesso di apposite:

↓

Policy recanti

a) Procedura di gestione dei data breach

e di uno specifico

b) Registro delle violazioni dei dati personali

Procedura per la gestione dei data breach

1. Se non è improbabile che vi sia un rischio per i diritti degli interessati, il Titolare deve effettuare – entro 72 h – apposita **notifica della violazione** al Garante per la protezione dei dati personali (art. 33, par. 1, GDPR)
2. La notifica al Garante può essere **preliminare** (cioè contenere solo gli elementi disponibili nell'immediato, da completarsi in seguito) o **completa** (vedremo in seguito).

Il **Titolare del trattamento** ha effettuato la **Notifica preliminare** al Garante entro le 72 h dalla conoscenza dell'evento?

Procedura per la gestione dei data breach

3. Se la violazione può comportare un **rischio elevato** per i diritti delle persone fisiche, il Titolare deve effettuare apposita **comunicazione della violazione** agli interessati, senza ingiustificato ritardo (art. 34, par. 1, GDPR)

4. La notifica agli interessati presuppone 2 valutazioni specifiche: a) la **valutazione del rischio** per gli interessati; b) la qualificazione del rischio per gli interessati come **elevato**.

Il **Titolare del trattamento** ha dato notizia della violazione in modo generale, in modo specifico o si è momentaneamente astenuto dal comunicare per verificare il rischio per gli interessati?

Procedura per la gestione dei data breach

5. A questo punto è necessario procedere con ulteriori specifici adempimenti, rivolti ad affrontare – in modo rispettoso della disciplina in materia di protezione dei dati personali – la violazione dei dati personali.

6. Questi adempimenti richiedono la collaborazione di tutti i servizi dell'organizzazione, non solo di quelli direttamente coinvolti.

7. Questi adempimenti sono – o dovrebbero essere - specificamente disciplinati in un documento interno, denominato Procedura per la gestione dei data breach.

Procedura per la gestione dei data breach

La prima attività da svolgere si sostanzia nella costituzione del TEAM di gestione del data breach.

Il TEAM a livello esecutivo deve essere composto da un numero ristretto di persone: 1 funzionario della segreteria organizzativa/generale (sotto la supervisione del Dirigente/Segretario); 1 funzionario del settore servizi informativi (sotto la supervisione del Dirigente); il DPO, qualora incaricato a tal fine.

Per operare correttamente è necessario che il TEAM possa rivolgersi e riferirsi a tutti i referenti dei diversi settori, che costituiscono il TEAM allargato e devono essere individuati in apposito elenco, per svolgere le attività che vado a descrivere.

Vi è a questo riguardo una vitale esigenza di chiarezza nei rapporti interni: da questo momento nessuna attività o comunicazione in materia di gestione del Data Breach deve essere fatta – in entrata o in uscita – senza coinvolgere il funzionario preposto della segreteria organizzativa/generale.

Procedura per la gestione dei data breach

Un data breach comporta la violazione dei dati personali trattati dal Titolare.

Tale violazione può riguardare, congiuntamente o disgiuntamente, 3 profili:

- Violazione della riservatezza (divulgazione/accesso non autorizzato/accidentale dei dati personali)
- Violazione della integrità (modifica non autorizzata/accidentale dei dati personali)
- Violazione della disponibilità (perdita, accesso o distruzione accidentale/non autorizzata di dati personali).

Procedura per la gestione dei data breach

Il primo compito del Titolare del trattamento di fronte ad un data breach è individuare il tipo di violazione che si è realizzata.

Quindi:

- Identificare la platea dei dati coinvolta dall'attacco e, in questo ambito, la platea di dati personali (volume);
- Identificare – anche per approssimazione – la platea degli interessati (quanti sono: decine, centinaia, migliaia ecc.);
- Identificare la tipologia di dati personali violati in ciascun ambito/settore.

Procedura per la gestione dei data breach

In questo momento – in ipotesi ricorrente – noi sappiamo che i dati personali violati sono stati crittografati e, pertanto, se ne è avuta una perdita di disponibilità, in parte temporanea (ed ora risolta?), in parte ancora persistente.

Ancora non sappiamo se i dati personali violati sono stati anche esfiltrati, e quindi si è verificato il rischio di perdita di riservatezza.

In ogni caso, in ciascuno dei settori coinvolti, è necessario identificare i 3 aspetti indicati, nel modo più preciso possibile: platea dei dati, platea degli interessati, tipologia dei dati personali violati.

Procedura per la gestione dei data breach

Il **secondo compito** del Titolare del trattamento è valutare il rischio per i diritti e le libertà degli interessati, sapendo che se il rischio è elevato è necessario comunicare agli interessati la violazione (NB: **solo agli interessati per cui il rischio si presenta elevato**).

La valutazione del rischio viene effettuata, sulla base delle informazioni fornite dai referenti dei settori e in collaborazione con loro, dal TEAM esecutivo e poi sottoposta a verifica dei vertici dell'azienda/ente, che su tale base individua il contegno da mantenere nei confronti degli interessati e nella notifica completa al Garante.

Procedura per la gestione dei data breach
La valutazione del rischio.

Per informazione:

La valutazione del rischio tiene conto dei seguenti criteri:

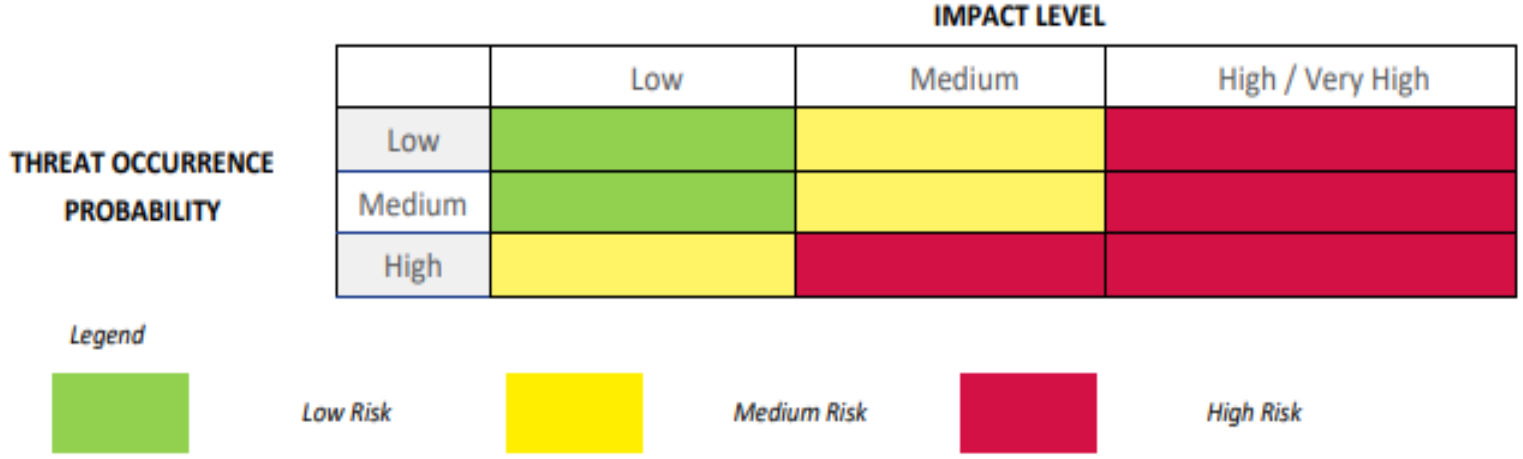
- il tipo di violazione (confidenzialità, integrità, disponibilità);
- natura, carattere particolare e volume dei dati personali;
- la facilità di identificazione delle persone fisiche sulla base dei dati violati;
- la gravità delle conseguenze per le persone fisiche a cui si riferiscono i dati violati;
- le caratteristiche particolari dell'interessato (es. minori);
- il numero delle persone fisiche interessate;
- eventuali contromisure adottate o da adottare per ridurre l'impatto della violazione.

Procedura per la gestione dei data breach
La valutazione del rischio

LIVELLO DI IMPATTO	DESCRIZIONE
BASSO	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.
MEDIO	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.
ALTO	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
MOLTO ALTO	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Procedura per la gestione dei data breach
La valutazione del rischio.

La matrice del rischio, che consente la qualificazione del rischio, deriva dalla correlazione fra probabilità e impatto:



Procedura per la gestione dei data breach
La valutazione del rischio.

Nel caso di Data Breach, la probabilità che il rischio si verifichi è una condizione soddisfatta: il rischio si è realizzato col data breach.

Pertanto ci si deve concentrare prevalentemente sul livello di impatto.

In ogni caso, le nozioni sin qui condivise sono al momento sufficienti per svolgere il lavoro che spetta a ciascuno, che di seguito sintetizzo per punti.

Il mio compito, al momento, è offrire supporto per ciascuno di questi punti.

Procedura per la gestione dei data breach
Attività da svolgere

	Competenza	Attività	Output
1	Segreteria organizzativa/generale	Istituzione TEAM data breach (esecutivo e allargato) Identificare i soggetti componenti	Documento con i componenti e referenti di settore
2	TEAM esecutivo + allargato	Condivisione con il TEAM delle attività da svolgere secondo la Procedura di gestione del Data breach Identificare le attività da svolgere e attribuirle ai soggetti competenti. Identificare i tempi di svolgimento delle attività.	Analisi attività da svolgere; condivisione Procedura di gestione del Data breach. **Adozione del calendario dei lavori e delle attività.**
3	TEAM esecutivo + allargato	identificare il perimetro dell'attacco e della violazione nei singoli settori	Documento interno dei singoli settori su: platea dei dati violati; 2. Platea degli interessati; tipologia dei dati violati.
4	TEAM esecutivo	Valutazione del rischio	Documento interno di valutazione dei rischi derivanti dalla violazione
5	TEAM esecutivo	Identificazione delle misure tecniche e organizzative adottate e da adottare	Documento interno di sintesi identificazione delle misure tecniche e organizzative appropriate ai rischi verificatisi

Procedura per la gestione dei data breach
Attività da svolgere

	Competenza	Attività	Output
6	TEAM esecutivo	Redazione relazione istruttoria sintetica	Relazione istruttoria
7	TEAM esecutivo + allargato	Presentazione e discussione relazione istruttoria	Riunione e modifiche alla relazione istruttoria
8	Segreteria generale + livello politico col supporto del TEAM esecutivo	Decisione in ordine alla adozione delle misure tecniche e organizzative	Adozione delle misure tecniche e organizzative
9	Segreteria generale + livello politico col supporto del TEAM esecutivo	Valutazione della esigenza e delle modalità di Comunicazione agli interessati	Comunicazione agli interessati
10	Segreteria generale + livello politico col supporto del TEAM esecutivo	Notifica completa al Garante	Redazione della notifica completa al Garante

Procedura per la gestione dei data breach
Tempi di azione

I tempi di azione.

Sono decisivi, ai fini della responsabilità giuridica dell'Azienda/Ente, di fronte al Garante (ed alle verifiche che possono essere richieste) e di fronte agli interessati (ed ai diritti che possono far valere, in ogni sede).

Dipendono, in prima battuta, dalle decisioni assunte in prima battuta dall'Azienda/Ente e queste decisioni (velocità e appropriatezza) dipendono, a loro volta, dal grado di organizzazione e di previsione dell'eventualità del data breach, in precedenza all'evento.

Procedura per la gestione dei data breach
Normativa rilevante

1. GDPR, artt. 32-34;
2. Gruppo art. 29, WP250rev.01 (2018), Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679;
3. ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, Working Document, v1.0, December 2013;
4. EDPB, Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali;
5. EPDB, Guidelines 9/2022 on personal data breach notification under GDPR;
6. Per approfondire: https://www.garanteprivacy.it/regolamentoue/databreach