Data breach privacy

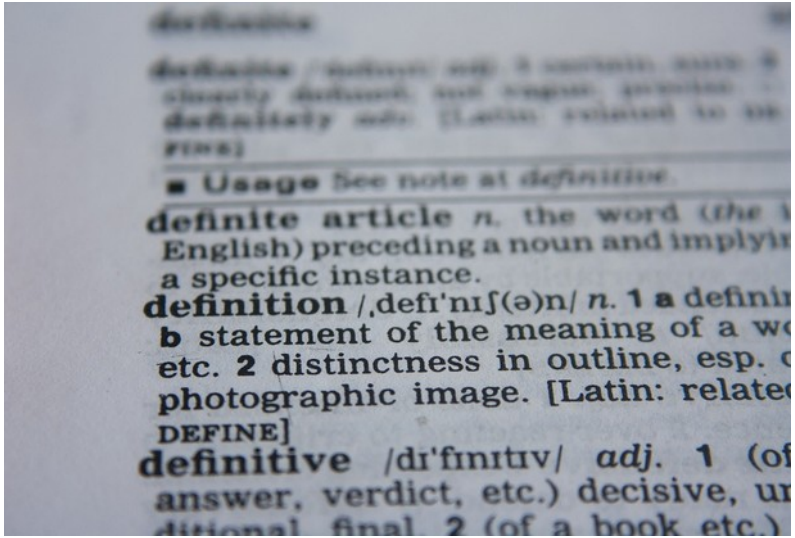
Cosa sono? Cosa fare e come?

Stefano Bendandi

Definizione di data breach

Cos’è un data breach?

- Secondo il Reg. Ue 679/2016 (GDPR) è una **violazione** della **sicurezza** dei dati personali conservati, trasmessi o trattati che ne comporta, in modo accidentale o illecito:
  - la **distruzione** o la **perdita**,
  - la **modifica**,
  - la **divulgazione** a terzi non autorizzati o l’accesso da parte di terzi non autorizzati



Confidenzialità, integrità e disponibilità

1. Divulgazione a terzi non autorizzati o accesso da parte di terzi non autorizzati significa **violazione** della caratteristica di **confidenzialità** del dato personale
2. Modifica significa **violazione** della caratteristica di **integrità** del dato personale (integrità come contenuto e come conservazione);
3. Distruzione o perdita significa **violazione** della caratteristica di **disponibilità** del dato personale

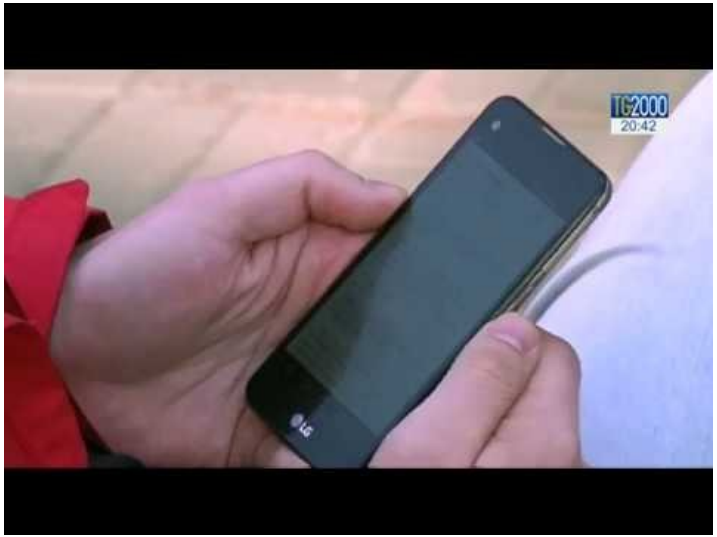
Esempi di data breach

- Non importa se la violazione è accidentale (es. errore) o intenzionale (es. attacco interno o esterno), ad esempio:
  - Accesso da parte di terzi non autorizzati ad un applicativo con cui si trattano dati personali,
  - Perdita o furto di documenti cartacei oppure di dispositivi rimovibili (es. chiavette usb, cd/dvd, ecc.) contenenti dati personali,
  - Invio di una email contenente dati personali a destinatari errati,
  - Cancellazione di file o database contenenti dati personali,
  - Modifica non voluta dei dati personali

Conseguenze di un data breach

- Le conseguenze di una **violazione** dei dati personali si valutano in relazione ai **diritti** e **libertà** delle persone interessate;
- Una violazione può produrre danni fisici, materiali o immateriali alle persone, ad es:
  - furto o usurpazione d'identità,
  - perdite finanziarie o altri danni di natura economica,
  - danni alla reputazione (es. iscrizione in black list finanziarie) o di natura sociale,
  - perdita di riservatezza dei dati protetti da segreto professionale (es. avvocato)

Cosa dice il garante della privacy



- L’autorità garante della privacy ha predisposto una pagina web dedicata al “data breach”;
- Nella pagina sono inclusi approfondimenti e linee guida da seguire, oltre a consigli su cosa fare in caso di violazione

Come gestire un data breach

Identificazione delle violazioni

- E’ la condizione necessaria per trattare correttamente una violazione
- Se non identifico le violazioni come posso trattarle?
  - Non posso...ne sono inconsapevole, ma la violazione rimane e con essa i rischi per le libertà e i diritti degli interessati e il rischio di sanzioni per il titolare
- La capacità di identificare le violazioni può dipendere da:
  - misure tecnologiche: controllo e monitoraggio delle infrastrutture informatiche, dei sistemi e flussi informativi
  - misure organizzative (es. procedure aziendali sulla gestione dei data breach)

Valutazione dei rischi di una violazione

- **Valutare** il rischio è indispensabile al titolare per decidere se **notificare** o meno la violazione;
- Il GDPR non prevede alcuna **metodologia** di **valutazione**;
- Il titolare ha la più ampia **libertà** di scegliere la metodologia che si adatta meglio al suo caso
- Ma deve poter **dimostrare** di aver valutato i rischi in modo **oggettivo**;
- E la sua scelta di notificare o meno deve essere **giustificabile**

Come valutare un data breach

Come valutare i rischi di un data breach

- Enisa (Agenzia Europea per la sicurezza delle reti ed informazioni) ha elaborato una proposta di **metodologia** per valutare la **severità** dei data breach
- Il concetto di **severità** di un data breach è coerente con quello di **rischio** del GDPR
- Si tratta della *stima dell'entità potenziale di una violazione dei dati*
- Nel documento sono inclusi appendici informative ed esempi pratici

Criteri di calcolo della severità del rischio

- I criteri proposti sono:
  - **DPC**: valuta la criticità dei dati personali in un contesto di trattamento,
  - **EI**: è un parametro di correzione del primo ed indica la facilità con la quale i dati permettono di identificare una persona,
  - **CB**: identifica le circostanze relative alla violazione
- La **formula** per il calcolo della **severità** del rischio è: **(DPC * EI) + CB**;

DPC - Contesto di elaborazione dei dati

1. **Classificazione** del tipo di **dati** personali violati (cfr. documento - Annex 1 - A1):
    a. Dati personali **comuni**,
    b. Dati personali **comportamentali**,
    c. Dati personali **finanziari**,
    d. Dati personali **sensibili**
2. Il punteggio attribuito al DPC può essere aumentato o diminuito se esistono fattori accrescitivi o diminutivi (cfr. documento - Annex 1 - A2/A3)

EI - Facilità di identificazione

1. Questo fattore esprime la **facilità** con cui chi ha accesso ai dati violati può **identificare** i soggetti **interessati**;
2. I **valori** sono stati distinti in quattro livelli (cfr. documento - Annex 2):
    a. **trascurabile**,
    b. **limitato**,
    c. **significativo**,
    d. **massimo**

CB - Circostanze della violazione

1. Questo fattore valuta il **tipo** di **violazione** (cfr. documento - Annex 3 - A1, A2, A3):
    a. perdita di **confidenzialità**: accesso ai dati personali da parte di chi non è autorizzato oppure per una finalità illegittima,
    b. perdita di **integrità**: l'informazione originaria è modificata e i dati sostituiti possono essere pregiudizievoli per gli interessati,
    c. perdita di **confidenzialità**: non è possibile accedere ai dati in modo temporaneo o permanente
2. E la presenza di un intento malevolo (cfr. documento - Annex 3 - A4)

Severità di un data breach - Tabella

Severità di un data breach = SE		
SE < 2	**Basso**	gli individui possono sperimentare piccoli inconvenienti superabili senza alcun problema (es. tempo occorrente per inserire nuovamente le informazioni, fastidio, irritazione, ecc.)
2 ≤ SE < 3	**Medio**	gli individui possono incontrare inconvenienti significativi superabili con alcune difficoltà (es. costi supplementari, indisponibilità di accedere a servizi, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.)
3 ≤ SE < 4	**Alto**	gli individui possono incontrare conseguenze significative superabili con gravi difficoltà (es. appropriazione indebita di fondi, inserimento in black list, danni alla proprietà, perdita del lavoro, chiamata in giudizio, peggioramento dello stato di salute, ecc.).
4 ≤ SE	**Elevato**	gli individui possono incontrare conseguenze significative o irreversibili, che potrebbero non essere in grado di superare (es. incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc).

Cosa fare in caso di data breach

Registrazione della violazione

- E’ un obbligo previsto dall’art. 33, par. 5 del GDPR: *il titolare del trattamento* ***documenta*** *qualsiasi* ***violazione*** *dei dati personali, comprese le* ***circostanze*** *a essa relative, le sue* ***conseguenze*** *e i* ***provvedimenti*** *adottati per porvi rimedio*
- L’obbligo vale anche in assenza di notifica e permette all'autorità di controllo di **verificare** il rispetto della norma
- La registrazione delle violazione è una **opportunità** per apprendere dagli errori e per disporre di serie storiche utili per valutare i rischi

Documentazione dei data breach

- In relazione alla norma è possibile ipotizzare un contenuto minimo che comprenda:
  - la descrizione delle **circostanze** della violazione di sicurezza,
  - le **conseguenze** della violazione di sicurezza, ossia i **rischi** per i **diritti** e le **libertà** degli interessati,
  - i **provvedimenti** adottati dal titolare per porre rimedio alla violazione (es. **misure** di **sicurezza** per mitigare i rischi)
- Non è previsto un termine minimo di conservazione del registro

Misure adottabili nei data breach

- Provv. Garante Privacy 30 aprile 2019:
  - il garante richiama le *Linee guida sulla notifica delle violazioni dei dati personali*, emanate dal gruppo di lavoro dell'art 29 e poi modificate
  - sulla base delle linee guida il garante ritiene che il titolare, in caso di data breach, debba **fornire** consulenza specifica ai soggetti interessati sul modo in cui **proteggersi** dalle possibili **conseguenze** della violazione
- Anche il considerando 86 del GDPR parla di **raccomandazioni** dirette all'interessato per **attenuare** i potenziali **effetti** negativi del data breach

Notifica della violazione all'autorità garante

- La notifica è obbligatoria, a meno che sia **improbabile** che la violazione presenti un **rischio** per i diritti e le libertà degli interessati
- Se la violazione è scoperta da un responsabile del trattamento quest'ultimo ne informa il titolare senza ritardo
- La notifica va fatta entro le 72 ore dalla scoperta della violazione; se fatta dopo questo termine deve contenere i motivi del ritardo

Contenuti minimi della notifica al garante

1. **descrizione** della natura della **violazione**, compresi le categorie e il numero approssimativo degli interessati e delle registrazioni dei dati interessati dalla violazione;
2. nome e dati di contatto del responsabile della protezione dei dati o di altro punto di contatto
3. **descrizione** delle **conseguenze** probabili della violazione;
4. **descrizione** delle **misure** adottate o da adottare per rimediare alla violazione o mitigarne gli effetti

Notifica agli interessati

- Se la violazione presenta un rischio elevato, la **notifica** va fatta anche ai singoli **interessati**, a meno che ricorra una delle seguenti eccezioni:
  - il titolare ha applicato ai dati personali violati **misure** tecniche ed organizzative **adeguate** per proteggerli, in particolare la cifratura dei dati
  - il titolare ha adottato successivamente misure per scongiurare un rischio elevato per i diritti e le libertà degli interessati
  - la comunicazione richiede sforzi **sproporzionati**: gli interessati sono informati con una comunicazione pubblica o un altra iniziativa simile
- I contenuti minimi sono quelli dei punti 2,3 e 4 della notifica al garante

Sanzioni e responsabilità

- L'**inadempimento** degli obblighi relativi ai *data breach* (art. 33 e 34) è soggetto ad una **sanzione** amministrativa pecuniaria fino a 10 mln € o, per le imprese, fino al 2% dell'ultimo fatturato mondiale annuo
- Inoltre, chiunque subisca un danno causato dalla violazione del GDPR può chiedere che gli venga risarcito
- Il titolare è esonerato da **responsabilità** soltanto se dimostra che il danno non gli è imputabile in alcun modo