Privacy: come gestire un data breach

Il data breach consiste in una violazione dei dati che determina la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati ai dati personali. È in definitiva un'anomalia che colpisce i dati dell'interessato, che fuoriescono da un archivio custodito e iniziano a circolare e a diventare pubblici. Il GDPR vuole che tali eventi siano comunicati al Garante della privacy e agli interessati: la mancata notifica espone l'azienda all'applicazione di elevate sanzioni. Come evitare il rischio di data breach? Quali misure è opportuno adottare?

Il Regolamento UE 2016/679 - **GDPR** in materia di protezione dei dati personali dedica una disciplina specifica al "**data breach**", ossia all'ipotesi di una **violazione dei dati** idonea a comportare – accidentalmente o come conseguenza di un illecito – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Si tratta dell'incubo peggiore previsto dal Legislatore europeo nella nuova società dell'informazione, dove anche **grandi piattaforme e server**/servizi custodiscono i dati di milioni di utenti con indirizzi e-mail, credenziali, indirizzi e numeri di carte di credito.

Una violazione di questi tipi di dati personali può, se non affrontata in modo adeguato e tempestivo, provocare **danni gravissimi** alle persone fisiche.

Tali danni possono consistere, ad esempio, nella **perdita del controllo dei dati** da parte degli interessati stessi, nella limitazione o soffocamento dei loro diritti, nella discriminazione nel contesto sociale dove vivono e lavorano, nell'usurpazione o nel furto di identità, in perdite finanziarie, nella decifratura non autorizzata della pseudonimizzazione, in un pregiudizio alla reputazione, nella perdita di riservatezza dei dati personali protetti da segreto professionale e, in generale, in tantissimi danni economici o sociali significativo.

Notifica al Garante

Per tale ragione, l'Articolo 33 del GDPR prevede che, in caso di violazione di archivi contenenti dati personali (ma, anche, in caso di smarrimento o furto di una chiavetta, di un hard disk esterno o di un computer portatile) il titolare del trattamento debba **notificare** la suddetta violazione **all'autorità di controllo competente** (ossia: al Garante) entro 72 ore dal momento in cui ne è venuto a conoscenza.

La comunicazione deve essere fatta anche a tutti gli utenti/interessati cui i dati si riferiscono, a meno che sia improbabile che quella violazione dell'archivio rappresenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale comunicazione deve essere accompagnata dalle ragioni del ritardo nell'agire in tal senso.

La notifica, in particolare, deve descrivere la natura della violazione, indicando – ove possibile – le categorie e il numero approssimativo dei dati personali violati e degli interessati coinvolti. Deve, inoltre, contenere il nome e i dati di contatto del responsabile della protezione dei dati o di un altro punto di contatto presso cui sia consentito ottenere più informazioni. Infine, deve descrivere le probabili conseguenze della violazione e le misure adottate, o di cui si propone l'adozione, al fine di porre rimedio alla violazione o di attenuarne i possibili effetti negativi.

Comunicazione all'interessato

Ai sensi dell'Articolo 34, poi, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe comunicarla senza indebito ritardo anche all'interessato stesso, consentendogli, in tal modo, di prendere le precauzioni necessarie.

La comunicazione dovrebbe descrivere la **natura della violazione** e contenere raccomandazioni per la persona fisica interessate dirette ad attenuare i potenziali effetti negativi (ad esempio: il suggerimento di cambiare immediatamente le credenziali). Essa, inoltre, dovrebbe essere effettuata non appena ragionevolmente possibile, in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti.

La comunicazione all'interessato non è tuttavia richiesta se si ravvisano una serie di **circostanze specifiche**.

La prima ricorre quando il titolare del trattamento ha messo in atto, e applicato ai dati che sono stati oggetto di violazione, tutte le necessarie misure tecniche e organizzative di protezione, comprese quelle destinate a rendere i dati personali incomprensibili ai soggetti non autorizzati (come, ad esempio, la cifratura delle informazioni).

La seconda è prevista quando il titolare del trattamento abbia successivamente adottato misure per scongiurare il verificarsi di un rischio elevato per i diritti e le libertà degli interessati.

La terza si presenta quando la comunicazione stessa richiederebbe **sforzi sproporzionati** e, in tal caso, si può procedere a una comunicazione pubblica o ad altra soluzione analoga, così da informare gli interessati in maniera ugualmente efficace.

In sostanza, dunque, è opportuno procedere a un duplice controllo.

Da un lato, occorre verificare che siano state adottate le **misure di protezione adeguate**, così da poter stabilire se c'è stata violazione dei dati personali e informare, di conseguenza, l'autorità di controllo e gli interessati. Dall'altro, si deve stabilire se la notifica è stata trasmessa senza ingiustificato ritardo, tenendo conto, in particolare, della natura e della gravità della violazione, nonché delle sue conseguenze ed effetti negativi per l'interessato.

Sanzioni

Il mancato rispetto dell'obbligo di notifica pone l'autorità di controllo nella condizione di poter applicare le sanzioni a sua disposizione. Queste possono consistere nell'**esercizio dei poteri** previsti dall'Articolo 58 del GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere i flussi di dati) e nell'imposizione di **sanzioni amministrative** ex Articolo 83, il cui importo può arrivare fino a 20 milioni di euro o, se superiore, al 4% del fatturato totale annuo dell'esercizio precedente.

Dato che l'obbligo di notifica spetta al titolare, è molto importante che, nell'affidare servizi a responsabili del trattamento, questi, preliminarmente, si accerti della **capacità del fornitore** nel gestire tempestivamente e adeguatamente un incidente di sicurezza e preveda, quindi, idonee clausole contrattuali, come stabilito

dall'Articolo 28, Paragrafo 3 del GDPR, che regolino il rapporto di fornitura in modo da garantire il rispetto del Regolamento stesso.

Considerazioni finali

Gli obblighi della notifica e della comunicazione, sebbene richiedano adempimenti specifici, non possono essere letti e interpretati correttamente senza considerare la loro correlazione con l'intero GDPR. In particolare, in tal senso, sono fondamentali gli Articoli 24 e 32 del GDPR, che impongono ad ogni titolare di:

1. mettere in atto misure tecniche e organizzative adeguate per garantire il rispetto del GDPR
2. essere in grado di dimostrare che il trattamento sia effettuato conformemente al GDPR
3. riesaminare e aggiornare tali misure quando necessario
4. garantire un **livello di sicurezza** adeguato al rischio.

Non si può, infatti, pensare di gestire correttamente un possibile data breach (soprattutto in una realtà complessa) se il lato organizzativo (istruzioni, dialogo tra le varie "parti" dell'azienda, chiarezza nei processi) non sia impeccabile.

Il data breach, nell'ottica dell'interessato – e ricordiamo sempre che l'interessato è posto al centro del Regolamento – è visto come **un'anomalia** che colpisce i suoi dati i quali, improvvisamente, fuoriescono da un archivio custodito e iniziano a circolare e a diventare pubblici. Ciò che la legge vuole è che questi eventi siano sia comunicati all'autorità che è in grado di intervenire da un punto di vista della verifica ed, eventualmente, delle sanzioni, sia agli interessati stessi, che hanno diritto di conoscere.

Si noti, anche in questo contesto, l'importanza della **cifratura degli archivi**: un data breach su un archivio di dati cifrato allo stato dell'arte può evitare grandi responsabilità in capo al titolare e annullare qualsiasi effetto dannoso dell'evento nei confronti di chiunque, titolare, interessati e terzi.