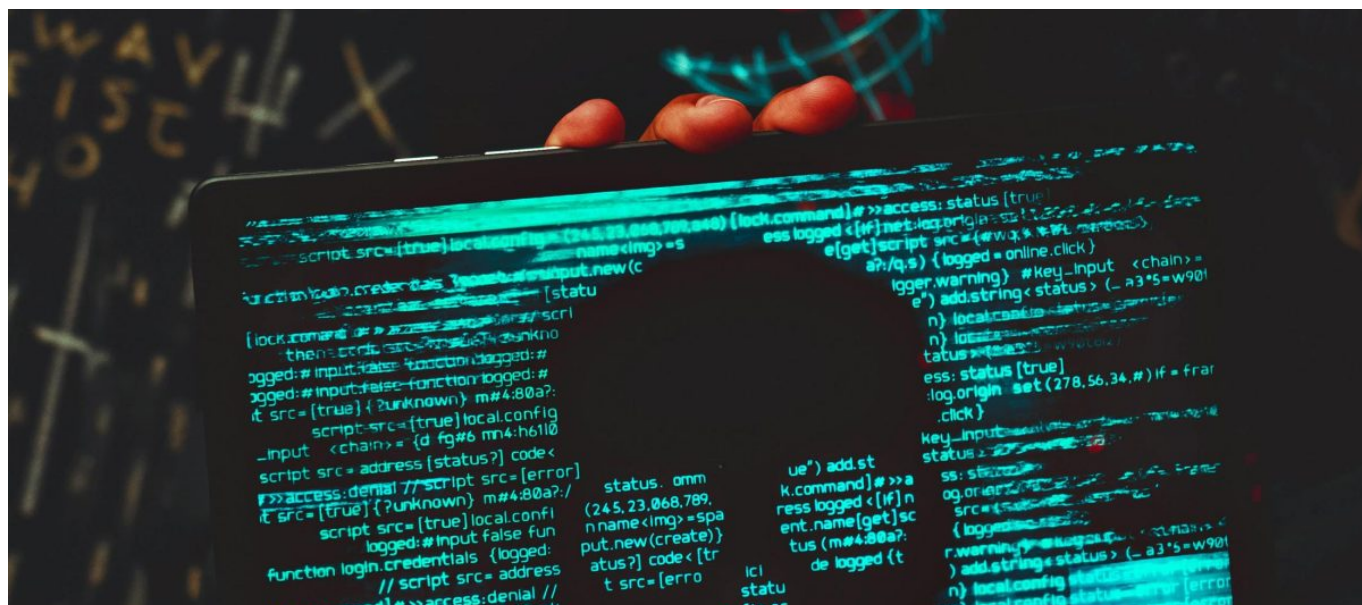




Data breach e GDPR: cosa devono fare le aziende nelle prime 72 ore

Posted on Marzo 9, 2026

Un data breach, ovvero una violazione dei dati personali, rappresenta uno dei rischi più rilevanti per le aziende che trattano informazioni di clienti, dipendenti o partner.

Il Regolamento generale sulla protezione dei dati (GDPR) impone obblighi precisi alle organizzazioni in caso di violazione dei dati. In particolare, le aziende devono agire rapidamente: in molti casi è necessario notificare il data breach all'autorità di controllo entro 72 ore.

Gestire correttamente le prime ore dopo una violazione è fondamentale per limitare i danni, rispettare gli obblighi normativi e proteggere la reputazione aziendale.

Che cos'è un data breach

Secondo il GDPR, un data breach è una violazione di sicurezza che comporta:

- accesso non autorizzato ai dati personali
- perdita o distruzione dei dati
- divulgazione accidentale di informazioni
- modifica non autorizzata dei dati

Queste violazioni possono derivare, ad esempio, da:

- attacchi informatici
- errori umani
- accessi non autorizzati ai sistemi aziendali
- smarrimento di dispositivi contenenti dati personali

Le prime azioni da intraprendere

Quando si verifica una violazione dei dati, l'azienda deve intervenire rapidamente per contenere l'incidente e valutarne l'impatto.

Tra le prime attività da svolgere vi sono:

- individuare la causa della violazione
- bloccare o limitare l'accesso ai sistemi compromessi
- raccogliere le informazioni sull'incidente
- identificare le categorie di dati coinvolti
- valutare i possibili rischi per le persone interessate

Una gestione tempestiva dell'incidente è essenziale per ridurre le conseguenze legali e operative.

L'obbligo di notifica entro 72 ore

Se la violazione comporta un rischio per i diritti e le libertà delle persone, il GDPR impone la notifica all'autorità di controllo competente entro 72 ore dal momento in cui l'azienda ne viene a conoscenza.

La notifica deve includere informazioni come:

- la natura della violazione
- le categorie e il numero approssimativo di dati coinvolti
- le possibili conseguenze della violazione
- le misure adottate o previste per affrontare l'incidente

In alcuni casi, l'azienda deve anche informare direttamente le persone interessate.

L'importanza di una procedura interna di gestione dei data breach

Per rispettare gli obblighi previsti dal GDPR, le aziende dovrebbero dotarsi di una procedura interna di gestione dei data breach.

Questa procedura dovrebbe definire:

- le responsabilità interne
- i processi di segnalazione degli incidenti
- le modalità di valutazione del rischio
- le procedure di notifica alle autorità

Un approccio strutturato consente di reagire in modo più efficace e di dimostrare la responsabilità e l'accountability dell'organizzazione.

Il ruolo della compliance integrata

La gestione dei data breach non riguarda solo la protezione dei dati. È spesso collegata ad altri ambiti di compliance aziendale, come:

- sicurezza informatica
- gestione dei rischi
- sistemi di controllo interno
- modelli organizzativi di compliance

Integrare le procedure GDPR con gli altri sistemi di controllo aziendale aiuta a rafforzare la prevenzione e la gestione degli incidenti.

Come Aria supporta le aziende

Aria supporta imprese ed enti pubblici nella gestione della compliance GDPR, aiutando le organizzazioni a sviluppare procedure efficaci per la prevenzione e la gestione dei data breach.

L'approccio integra la protezione dei dati con i sistemi di compliance aziendale, tra cui Modello 231 e anticorruzione, per costruire un sistema di controllo coerente e sostenibile.