Come riconoscere e notificare il data breach dello studio

La privacy. I professionisti dell'area economico-giuridica gestiscono informazioni sensibili dei clienti
Anche la perdita di Pc o telefoni può tradursi in una violazione del regolamento Ue da segnalare al Garante

Aurora Agostini

Il rischio di violazioni informatiche è sempre più frequente: basti pensare all'ultimo caso di cronaca, con le migliaia di accessi illegittimi ai conti correnti bancari di personaggi famosi da parte di un dipendente di Intesa Sanpaolo. Anche per i professionisti è cruciale comprendere a fondo il fenomeno del data breach, le sue implicazioni e gli obblighi che ne derivano. La crescente digitalizzazione dei servizi professionali rende questo tema particolarmente rilevante per chi gestisce dati (anche sensibili) dei propri clienti.

Riconoscere un data breach

Un data breach si verifica quando i dati personali subiscono una compromissione accidentale o illecita, che può portare alla loro distruzione, perdita o accesso non autorizzato. Per i professionisti, che sono titolari del trattamento dei dati personali dei propri clienti (e talvolta anche responsabili dei dati trattati per conto di questi ultimi) riconoscere tempestivamente questi eventi è fondamentale. Segnali come accessi non autorizzati ai sistemi, attività anomale su database o malfunzionamenti nei sistemi di sicurezza possono indicare una possibile violazione: un monitoraggio costante delle attività sui sistemi informatici diventa quindi non solo utile, ma essenziale per individuare e gestire prontamente eventuali problemi.

Notificare il data breach

Il Regolamento generale sulla protezione dei dati (Gdpr) stabilisce precise regole in caso di data breach. Se la violazione presenta rischi per i diritti e le libertà degli interessati, è necessario notificarla al Garante della privacy entro 72 ore dalla sua scoperta: questa notifica deve essere dettagliata, includendo informazioni sulla natura della violazione, il numero di persone coinvolte, le probabili conseguenze e le misure adottate per mitigare i danni. Tuttavia, anche quando si ritiene che la violazione non presenti rischi significativi, è importante documentarla accuratamente, in linea con il principio di accountability. Nei casi più gravi, oltre al Garante, vanno informati anche gli interessati, come previsto dall'articolo 34 del Gdpr.

Come mitigare i rischi

Le responsabilità dei professionisti in materia di protezione dei dati vanno ben oltre la semplice notifica in caso di violazione. È fondamentale implementare misure tecniche e organizzative adeguate, come la segregazione e la cifratura dei dati, mantenere un registro delle attività di trattamento, effettuare valutazioni d'impatto sulla protezione dei dati per i trattamenti più rischiosi e, in alcuni casi, nominare un Responsabile della protezione dei Dati (Dpo). Ad esempio, la nomina del Dpo è necessaria quando lo studio tratta una quantità significativa di dati personali, specialmente dati sensibili o giudiziari, oppure quando agisce come responsabile del trattamento per conto di grandi aziende o enti pubblici.

La prevenzione gioca un ruolo chiave: adottare una solida politica di sicurezza informatica che includa l'uso di sistemi di crittografia, l'autenticazione a due fattori, backup regolari e aggiornamenti frequenti dei software è essenziale. Queste misure, unite a una formazione periodica del personale sulle migliori pratiche di sicurezza e sulle procedure da seguire in caso di data breach, possono significativamente ridurre il rischio di violazioni.

La diffusione capillare di tablet e smartphone ha introdotto nuove e significative vulnerabilità: la loro natura portatile li rende particolarmente suscettibili a perdite o furti, eventi che possono facilmente tradursi in un data breach. In questi casi, è cruciale agire rapidamente attivando procedure di blocco e cancellazione remota dei dati, cambiando le password degli account potenzialmente compromessi e, se necessario, notificando l'evento al Garante e ai clienti coinvolti.

La gestione efficace dei data breach e la conformità al Gdpr offrono ai professionisti non solo compliance alla normativa, ma anche un vantaggio competitivo, perché l'approccio proattivo rafforza la fiducia dei clienti, dimostrando impegno nella protezione di informazioni personali, inclusi dati sensibili come quelli sanitari o giudiziari. Le sanzioni per non conformità possono raggiungere i 20 milioni di euro o il 4% del fatturato annuo globale, ma il danno reputazionale rappresenta un rischio ancora maggiore per la stabilità del business.

PAROLA CHIAVE

#Data breach

Il data breach è una violazione della 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 trattati. Tra gli esempi: il furto o la perdita di dispositivi informatici; la perdita di dati personali a causa di incidenti, incendi o altre calamità; la divulgazione non autorizzata dei dati personali.