AU Acquirente Unico

DATA BREACH: VIOLAZIONI DI DATI PERSONALI, RISCHI PER GLI INTERESSATI E IMPATTI SULL'ORGANIZZAZIONE

COS'È UN DATA BREACH

Un data breach consiste nella 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 trattati. Per evitarlo, occorre valutare e adottare misure di sicurezza di tipo organizzativo, di tipofisico e di tipo logico che siano adeguate a minimizzare i rischi per i diritti e libertà degli interessati.

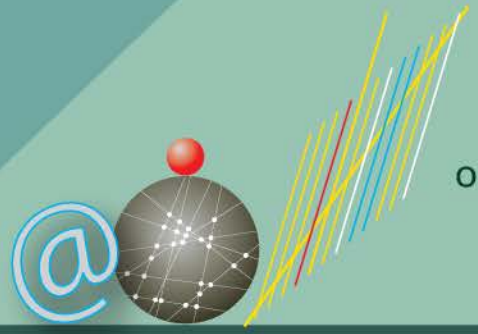
Infografica a cura di Digital & Law Department srl DIGITAL&LAW con il contributo scientifico dello Studio Legale Lisi STUDIO LEGALE LISI

AU Acquirente Unico

LE VIOLAZIONI DI DATI PERSONALI

Le violazioni possono essere classificate in base ai seguenti principi di sicurezza delle informazioni:

- Violazione di riservatezza: in caso di accesso o divulgazione, non autorizzati o accidentali, ai dati personali;
- Violazione di integrità: in caso di alterazione non autorizzata o accidentale dei dati personali;
- Violazione di disponibilità: in caso di perdita accidentale o non autorizzata di disponibilità, definitiva o temporanea, dei dati personali.



Infografica a cura di Digital & Law Department srl DIGITAL&LAW con il contributo scientifico dello Studio Legale Lisi STUDIO LEGALE LISI

AU Acquirente Unico

ESEMPI IN CUI SI VERIFICA UNA VIOLAZIONE DI DATI PERSONALI

- Invio di una comunicazione email contenente dati personali di terzi a destinatari errati (violazione di riservatezza)
- Modifica di dati personali in un data base da parte di un operatore autorizzato per scopi o vantaggi personali estranei allo svolgimento di mansioni lavorative (violazione di integrità)
- Impossibilità, anche temporanea, di accedere ai dati per attacchi informatici che veicolano virus ransomware e cryptolocker (violazione di disponibilità)

Infografica a cura di Digital & Law Department srl DIGITAL&LAW con il contributo scientifico dello Studio Legale Lisi STUDIO LEGALE LISI

AU Acquirente Unico

PROCEDURE PER GESTIRE I DATA BREACH E PUNTI DI ATTENZIONE

• Proteggere sempre i dati personali
con adeguate misure di sicurezza,
tecniche e organizzative, sia che i dati siano gestiti
in modalità cartacea, che informatica

• Adottare una specifica Policy per l'utilizzo delle risorse e degli strumenti
informatici aziendali, organizzando apposite sessioni formative per il personale

• Adottare una Procedura interna per la gestione delle violazioni di dati personali
che individui con chiarezza quali siano le figure che devono essere prontamente avvisate
e coinvolte all'interno dell'organizzazione aziendale (compreso ovviamente il DPO)
in caso di violazione, accertata o presunta, dei dati personali trattati

• Predisporre un Registro delle violazioni, in cui documentare tutti i data breach:
a prescindere dalla notifica all'Autorità Garante o dalla comunicazione agli interessati, infatti, il titolare del trattamento
deve documentare la violazione in un apposito registro,
al fine di consentire all'Autorità di effettuare eventuali controlli sul rispetto della normativa

Infografica a cura di Digital & Law Department srl DIGITAL&LAW con il contributo scientifico dello Studio Legale Lisi STUDIO LEGALE LISI

AU Acquirente Unico

COINVOLGIMENTO DEL DPO SECONDO IL GDPR

Il DPO dell'organizzazione

deve essere prontamente coinvolto:

- nella valutazione del rischio e nella scelta e nell'adozione delle misure di sicurezza tecniche e organizzative adeguate a garantire un livello di sicurezza commisurato al rischio di trattamento (art. 32 GDPR)
- in caso di data breach, per la valutazione circa la necessità della notifica all'Autorità di controllo o della comunicazione agli interessati (artt. 33 e 34 GDPR)

Infografica a cura di Digital & Law Department srl DIGITAL&LAW con il contributo scientifico dello Studio Legale Lisi STUDIO LEGALE LISI