

GDPR, 7 cose che le aziende devono sapere

Sette cose che le aziende devono sapere a proposito del nuovo regolamento europeo sulla data protection (GDPR).

1. Il GDPR riguarda tutte le aziende

Il GDPR riguarderà tutte le imprese a livello globale che processano i dati dei cittadini della Ue. Per la prima volta, la Commissione Europea esporta in tutto il mondo dei principi europei sulla data protection. Ciò significa che tutte le informazioni che riguardano i cittadini dell'Unione Europea dovranno rispettare le richieste del GDPR, rendendo così il regolamento Ue la prima legge globale sulla data protection.

2. Il GDPR amplia la definizione di dato personale

Il regolamento allarga la portata della definizione di dato personale. Il GDPR considera dati personali tutti i dati che possono servire ad identificare un individuo compresi, per la prima volta, i dati genetici, mentali, culturali ed economici o sociali.

3. Il GDPR rafforza le norme per ottenere un consenso valido all'uso di informazioni personali

La prova del consenso valido all'utilizzo dei dati personali sarà una delle sfide maggiori presenti nel GDPR. Aziende e organizzazioni dovranno assicurare un linguaggio semplice quando domandano il consenso alla raccolta di dati personali.

Dovranno essere chiare sulle finalità dell'uso dei dati personali, e dovranno accettare il fatto che silenzio e inazione non rappresentano più un consenso.

Senza la prova di consensi chiari le autorità potranno chiudere le attività di elaborazione dei dati personali.

4. Il GDPR rende obbligatoria la nomina del DPO nella PA e nelle imprese

Il GDPR impone la nomina del DPO (Data protection officer) nella PA e per tutte le organizzazioni che trattano dati personali come attività principale o che richiedono il monitoraggio di grandi quantità di dati o che processano dati su larga scala che riguardano determinate categorie di persone. Secondo stime dell'IAPP (International Association of Privacy Professionals) saranno almeno 28mila i DPO che verranno assunti entro l'entrata in vigore del nuovo regolamento in Europa. In Germania la nomina di un DPO è obbligatoria per le aziende con più di 10 dipendenti, ma questa figura professionale prenderà piede anche nelle imprese con meno dipendenti che processano grandi quantitativi di dati.

5. Il GDPR introduce l'obbligo del Privacy impact assessment

L'obbligo del Privacy impact assessment nel GDPR dipende in larga misura, secondo gli analisti, dall'influsso del Garante britannico. Di fatto, il GDPR richiede ai controllori della privacy in azienda di condurre valutazioni di impatto per tutte le attività a rischio di attacchi e falle per minimizzare appunto il rischio di perdite o furti di dati. La compliance dovrà essere garantita dal DPO in riferimento a tutti i progetti che coinvolgono l'utilizzo di dati personali.

6. Il GDPR introduce termini comuni per la notifica dei data breach

Il Gdpr armonizza le diverse leggi europee sulle notifiche in materia di Data breach.

La regolazione richiede che le organizzazioni devono notificare alle autorità locali i data breach entro 72 ore dall scoperta della falla. Ciò implica che aziende e organizzazioni abbiano a disposizione tecnologie per scoprire e rispondere ai dati breach in tempi stretti.

7. Il GDPR introduce il diritto all'oblio

Il GDPR introduce regole stringenti sul diritto all'oblio. Il principio di base riguarda la minimizzazione dei dati conservati dalle organizzazioni, l'obbligo di non cambiare in corso d'opera lo scopo per il quale i dati sono stati raccolti.

Ciò implica che per ogni utilizzo dei dati diverso dall'originale sarà necessario ottenere un nuovo consenso dei soggetti⁹ coinvolti. Le aziende dovranno quindi disporre di tecnologie per cancellare in tempo reale dati su richiesta dei soggetti.

GDPR, 7 cose che le aziende devono sapere