PRIVACY
Guida rapida

Strumenti per imprese e professionisti, consigli pratici sulla protezione dei dati, obblighi e adempimenti, sanzioni: guida rapida al GDPR in attesa del decreto di armonizzazione con il Codice Privacy.

GDPR: controllo dei dati ai cittadini

GDPR al via in Italia: da oggi tutte le pubbliche amministrazioni, le imprese, i professionisti e gli enti privati che trattano dati personali di cittadini UE su larga scala devono essere in regola con il nuovo Regolamento europeo sulla **Privacy**.
Il **Garante** mette a disposizione guide, moduli, istruzioni e tutorial per l'**auto-valutazione** dei rischi. Un consiglio: l'Authority britannica (ICO – Information Commissioner's Office) offre una guida e una serie di **test** per valutare il proprio sistema di protezione dati, con **check-list** specifiche per le diverse attività e funzioni aziendali.

Quadro normativo
Il riferimento normativo è il *Regolamento UE 2016/679* composto da 99 articoli, in vigore in tutti gli stati UE dal 25 maggio 2018.

Codice Privacy: cosa resta in vigore
Il decreto attuativo di **armonizzazione** con la legge italiana, che doveva essere approvato entro lo scorso 21 maggio, è invece slittato al **21 agosto**: la mancanza di norme di coerenza rischia quindi di creare confusione sugli **adempimenti**. Questo perché, fino all'approvazione del decreto, si sovrapporranno le disposizioni del **codice privacy** italiano e le direttive europee, anche se novità, ad esempio quelle in tema di data breach e responsabile dei dati, non trovano incongruenze.

Cosa cambia

GDPR in vigore dal 25 maggio: cosa cambia
Il primo passo da compiere, per ogni azienda o professionista, è quello di valutare, in base ai criteri indicati nel regolamento, l'adeguatezza di **infrastrutture** e **procedure**. In linea generale, una grande azienda deve adempiere a tutti gli **obblighi** previsti (nomina DPO, tenuta registro, adeguamento informative, misure contro il data breach, comunicazione al Garante…), mentre per le piccole realtà gli adempimenti sono meno stringenti. Di seguito alcuni **chiarimenti** e **consigli pratici**.

Dati personali
Secondo la definizione contenuta nel GDPR si tratta di: «qualsiasi informazione riguardante una persona fisica identificata o identificabile» direttamente o indirettamente, ad esempio attraverso nome, numero di identificazione, ubicazione, identificativo online, elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Per quanto riguarda gli **identificativi online**, spiega inoltre la Guida di Conflavoro PMI, i riferimenti sono: indirizzi IP, cookies, tag.

Protezione dei dati
Il regolamento fornisce linee guida per la protezione dei dati in termini di infrastrutture IT e procedure di sicurezza. Vanno previsti:

- pseudonimizzazione e cifratura dei dati;
- garanzia di riservatezza, integrità, disponibilità e resilienza di sistemi e servizi di trattamento;
- disponibilità, accesso ai dati personali e capacità di ripristino tempestivo in caso di incidente fisico o tecnico;
- test, verifica e valutazione periodica delle misure tecniche e organizzative adottate per la sicurezza del trattamento.

Responsabilità
- Il **titolare del trattamento** è l'azienda, lo studio o il professionista.
- Il **responsabile del trattamento** è invece la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
- Il **responsabile della protezione dei dati** (DPO) è il responsabile della misure di protezione; figura introdotta dal **GDPR** e obbligatoriamente nominata da chi gestisce dati sensibili su larga scala (sempre le pubbliche amministrazione e le grandi aziende, in casi specifici le PMI).

Registro trattamenti
Si tratta di un nuovo obbligo previsto dal GDPR per imprese sopra i 250 dipendenti. Se però l'azienda o lo studio o anche l'attività del libero professionista riguardano dati sensibili oppure il trattamento presenta un rischio per la protezione dei dati stessi, è obbligatorio indipendentemente dalla dimensione dell'organizzazione. Il registro contiene informazioni dettagliate su policy, procedure e standard di sicurezza adottati al fine di garantire la sicurezza e la protezione dei dati personali.

Comunicazioni al Garante
Oltre a comunicare gli estremi del DPO laddove richiesto, è necessario segnalare qualsiasi evento che possa rappresentare un rischio e, in caso di violazione (data breach) dei dati – con conseguente perdita, distruzione o indebita diffusione - bisogna immediatamente notificare l'accaduto al Garante.

Consenso
Il tradizionale consenso informato dell'interessato diventa più articolato: non solo deve sempre essere richiesto all'interessato ma prevedere anche specifiche modalità di formulazione ed essere espresso in maniera altrettanto chiara e inequivocabile. Soprattutto in relazione alle finalità del trattamento (es.: scopi commerciali) e alla possibilità di accesso e/o cancellazione dei dati stessi.

Sanzioni
In caso di inottemperanza alle direttive del regolamento, le multe possono essere salatissime. Le sanzioni possono arrivare fino al 4% del fatturato globale annuo.
- L'omessa o inesatta informativa sulla privacy costa da 6mila a 36mila euro,
- la mancata o infedele notificazione da 20mila a 120mila euro.