Dati personali

Secondo la da 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 mancato o infedele notificazione da 20mila a 120mila euro.