



## IL NUOVO REGOLAMENTO SULLA PRIVACY

Il 25 Maggio entra a pieno regime il nuovo regolamento europeo n.679/2016 sulla protezione dei dati delle persone fisiche ed al trattamento degli stessi, immediatamente applicabile in tutti gli stati della UE.

Tutte le aziende devono adeguarsi ai nuovi e più stringenti dettami della normativa europea, sia per quanto riguarda il trattamento dei dati personali dei propri dipendenti, sia per quanto riguarda quello dei clienti e dei potenziali clienti, se ed in quanto persone fisiche (le aziende sono escluse dalla tutela prevista da questa normativa).

Più specificatamente, ogni azienda deve opportunamente procedere ad una analisi preventiva del proprio stato rispetto agli obblighi previsti, secondo il principio dell'accountability (responsabilizzazione), in base al quale vanno posti in essere tutta una serie di adempimenti concreti, mirati a soddisfare la tutela dei dati, verificabili nei fatti e non solo sulla carta.

I due principi ulteriori introdotti sono quello della privacy by design e privacy by default, in pratica le aziende fin dall'inizio e ancor prima di ricevere un dato personale, devono strutturarne l'utilizzo e la conservazione in un'ottica di sicurezza per poi continuare ad applicarla nel tempo.

La sicurezza dei dati contro la possibile perdita/furto, diventa cioè parte integrante dei processi aziendali, non esistono infatti più misure minime idonee generalizzate, ma ogni singola azienda deve individuare di volta in volta le misure tecniche ed organizzative maggiormente adeguate, configurando quindi un nuovo approccio rispetto ad oggi.

Ulteriori novità introdotte sono il diritto all'oblio e la portabilità dei dati, il diritto cioè della persona a chiedere che i dati vengano rettificati o anche cancellati se non più necessari per le finalità per cui erano stati raccolti ed il diritto di chiedere ed ottenere che la trasmissione dei dati sia diretta da un titolare ad un altro.

Viene anche introdotto l'obbligo del data breach, l'obbligo per le aziende di notificare all'autorità del Garante, entro 72 ore, l'eventuale smarrimento o, peggio, furto (ad esempio hacker informatico), di informazioni detenute dall'azienda e riferite a persone fisiche.

In caso di trattamento su "larga scala" di dati personali od in caso di aziende con più di 250 dipendenti, i datori di lavoro hanno l'obbligo di nominare un Data Protection Officer (DPO), persona esterna con particolare conoscenza normativo-tecnica della materia, che sorvegli l'osservanza del regolamento da parte del titolare, del responsabile e degli incaricati.

Attenzione che le sanzioni previste sono enormi, si va dal 4% del fatturato globale, fino a 20 milioni di euro.

Si ricorda che tutte le circolari predisposte sono anche direttamente scaricabili dal sito [www.studioboller.it](http://www.studioboller.it) nella sezione riservata alle aziende.

L'argomento è stato qui trattato volutamente in modo sintetico e semplificato ad uso esclusivo dei clienti dello studio. Si rimane a disposizione per ogni eventuale ulteriore approfondimento e si porgono cordiali saluti