

ARRIVA IL REGOLAMENTO!

Le nuove norme per la protezione dei dati personali in breve

Fare il punto nave

Ogni organizzazione, come prima attività, deve verificare e analizzare tutti i documenti prodotti nel corso degli anni per la privacy. Chi gestisce l'infrastruttura informatica dovrà fornire ai consulenti o ai referenti interni il censimento del sistema informativo. Solo così si potrà effettuare una corretta analisi dei rischi indispensabile per ottemperare ad uno degli obblighi previsti dalle nuove norme. Tutte le aree coinvolte nel cambiamento di approccio, dall'EDP al Personale, al Marketing, senza escludere l'Amministrazione.

Documentare

Necessario che ogni nuovo passo realizzato venga documentato: i documenti devono sempre essere aggiornati.

Fare formazione

Il personale dovrà ricevere formazione mirata su casi concreti che incontra quotidianamente in base al proprio profilo professionale. In difetto di ciò previste sanzioni salate, anche fino a 10 milioni di euro.



© Burton Holmes - Giochi Olimpici di Atene 1896

Di corsa sulla stessa strada

Il 25 maggio 2018 entra in vigore il Regolamento UE 2016/679. Si tratta di un cambiamento significativo degli obblighi di adempimento alle norme che riguardano la protezione dei dati personali: quello che in molti continuano a chiamare *privacy*.

Valutare con attenzione gli obblighi

Gli obblighi non sono i medesimi per tutti: alcune organizzazioni dovranno scegliere un Responsabile Protezione Dati (o *Data Protection Officer*) a cui affidare il compito di controllare e sorvegliare le attività di adeguamento facendo la formazione ai dipendenti e consigliando le priorità su cui focalizzare le attività di miglioramento. Il DPO però non potrà compiere tali attività in prima persona: le attività di adeguamento dovranno anche coinvolgere i vari uffici del titolare, nessuno escluso.

Gli obblighi “minimi”

In ogni caso quasi tutte le organizzazioni dovranno:

- Tenere un registro dei trattamenti dove vengono indicati i trattamenti di dati personali e i passi logici, informatici e giuridici dei trattamenti;
- Indicare le misure di sicurezza adottate a seguito di analisi dei rischi;
- Redigere un documento in forma di parere dove si sceglie motivatamente perché avvalersi (o meno) di un DPO;
- Revisionare tutte le informative e le raccolte di consensi.

Cosa si deve certamente fare...

Devono essere rivisti: i contratti con i fornitori, quando è previsto uno scambio di dati personali; tutte le informative realizzate nel corso degli anni e i moduli di raccolta del consenso: cambiano le regole e quindi i testi da inserire in questi documenti.

E le sanzioni? Fino al 4% del fatturato annuo

Le sanzioni continuano ad esistere, anzi, il Regolamento ha apportato una modifica sostanziale al sistema sanzionatorio: non saranno più comminate in base al tipo di violazione ma calcolate fino al 4% del fatturato annuo del trasgressore.

Qui di seguito un quadro minimo delle sanzioni previste ad oggi.

Il regolamento è applicato **in modo uguale** in tutta l'UE, senza che sarà necessaria alcuna legge di recepimento nazionale.