



**Dott. Giovanni Prudenzano**

Consulente del lavoro - Consulente aziendale

**Dott. Anna Monica Montanaro**

Dottore Commercialista - Revisore Contabile

Circolare 5/2018 del 22.05.2018

*Ai gentili Clienti*

**Informativa: Regolamento UE 679/2016 in materia di Privacy. Entrata in vigore 25 maggio 2018.**

Gentile Cliente,

come noto, dal prossimo 25 maggio 2018 troverà piena applicazione la nuova normativa in materia di privacy con il Regolamento UE 2016/679 (GDPR) che andrà a sostituire l'attuale Codice della Privacy (D.lgs. 196/2003) comportando per TUTTE le Aziende (senza distinzione di attività ed anche le aziende senza dipendenti) l'obbligo di mettere in atto nuove e complesse misure tecniche ed organizzative per essere in grado di dimostrare che il trattamento dei dati è effettuato conformemente al Regolamento.

Il Regolamento impone a tutte le Aziende un cambiamento profondo nella gestione della privacy poichè, diversamente dal passato, oggi viene posta a carico del titolare la responsabilità (c.d. principio di Accountability) di definire, dopo l'analisi dei rischi, le misure di sicurezza idonee a garantire la privacy dei dati personali trattati dal Titolare e la responsabilità per la verifica della loro efficacia. Obblighi che prevedono un riesame ed aggiornamento costante di tutte le misure di trattamento e protezione dei dati personali attuate in azienda.

In caso di violazione delle nuove norme verranno applicate pesanti sanzioni che potranno arrivare a 20 milioni di euro, ovvero fino al 4% del fatturato oltre a rilevanti azioni di risarcimento dei danni a carico dell'Azienda.

La complessità degli obblighi imposti dal Regolamento UE 679/2016 per le Aziende e relative sanzioni hanno portato varie strutture a pubblicare checklist o software di gestione della norma .

Tuttavia appare evidente come la mera compilazione della checklist (o soli software) non deve essere intesa come strumento sufficiente per ottenere la conformità dell'organizzazione dell'Azienda alle disposizioni del

GDPR richiedendosi l'attuazione di tutto quanto previsto che, peraltro, varia a seconda delle peculiarità e specifiche attività svolte in ogni azienda che rendono difficile la standardizzazione degli adempimenti.

Quindi assolutamente diffidate di adempimenti meramente documentali o a distanza.

Ciò premesso, considerata la complessità degli adempimenti normativi del GDPR e delle sanzioni previste, al fine di consentire a tutte le Aziende di avere un minimo dettaglio degli obblighi imposti dal nuovo regolamento UE si elencano a mero titolo esemplificativo e non esaustivo i principali adeguamenti:

- Classificazione dei Dati Personali
- Classificazione dei Trattamenti
- Valutazione del rispetto dei Principi Privacy
- Definizione contrattualistica, informative aziendali conformi al Regolamento UE 679/2016
- Progettazione nel rispetto della Privacy by Design e Privacy by Default
- Valutazione d'impatto sulla protezione dei dati
- Definizione delle misure di sicurezza
- Redazione del Manuale del Sistema di Gestione Privacy
- Adozione di Codici di Condotta Privacy
- Tenuta del Registro delle attività di trattamento (Registro Privacy)
- Nomina del Responsabile della Protezione dei Dati (Privacy Officer) (eventuale)
- Redazione di contratti per disciplinare i rapporti di Contitolarità
- Redazione delle nomine dei Responsabili del Trattamento Dati
- Redazione di informativa privacy
- Redazione di procedure per la violazione dei dati personali (Data Breach)
- Redazione di procedure per l'esercizio dei Diritti dell'Interessato
- Adempimento degli obblighi privacy in materia di Profilazione
- Consultazione Preventiva, Comunicazioni e Notifiche al Garante Privacy

Si ribadisce il suggerimento di non affidarsi a soggetti che offrono meramente software di gestione o supporto documentale: **è necessario fare analisi aziendale e valutazione.**

Certi del Vostro interesse Vi salutiamo e restiamo a disposizione per ogni possibile chiarimento.

Cordiali Saluti.

Per Studio Format

f.to Dr. Prudenzero Giovanni Antonio