

17. Consulenza Privacy e REGISTRO DEI TRATTAMENTI (UE 679/2016 – GDPR D.LGS. 101/2018)

Il 25 Maggio 2018 è entrato ufficialmente in vigore il nuovo [Regolamento Europeo UE 2016/679 -GDPR](#) che impone a tutte le aziende all'interno della UE, quindi Italia compresa, di adottare nuove misure per la **protezione dei dati** e per la **Privacy**.

Rispetto al Codice della Privacy del 2003 D.Lgs.196, introduce nuove figure come il **DPO** (*Data Protection Officer o Responsabile della Sicurezza*) e modifica ruoli e responsabilità degli attuali **Titolari** e **Responsabili del Trattamento**.

Viene introdotto l'obbligo di **denunciare** alle autorità competenti **qualsiasi perdita** o **inaccessibilità anche parziale dei dati** e di **documentare** tutte le misure adottate per rendersi **adeguati** al regolamento (**Data Breach**).

Il Regolamento prevede inoltre un inasprimento delle **sanzioni** sia **amministrative** che **penali** che potranno arrivare fino a 20 Milioni di Euro o il 4% del fatturato.

Il GDPR richiede al **titolare una forte responsabilizzazione** sul trattamento dei dati effettuati e introduce una sostanziale inversione della prova: per non rispondere del danno emergente da trattamenti non leciti occorre dimostrare di aver fatto tutto il possibile per evitarlo.

Alle società è richiesto di prendere in considerazione prima di tutto, **i diritti di tutela e riservatezza di ogni soggetto**, progettando tutto intorno alla persona fisica; in altre parole tutti i processi aziendali devono essere seguiti e progettati considerando adeguatamente la protezione dei dati personali (**Privacy by Design**).

Gli step necessari e finalizzati all'adozione delle misure adeguate al nuovo Regolamento EU-GDPR sono sostanzialmente:

- Effettuare un'analisi dei rischi puntuale e precisa (DPIA)
- Nominare i Responsabili del Trattamento e se previsto il Data Protection Officer (DPO)
- Documentare le misure adottate e tenerle aggiornate
- Adeguare l'infrastruttura
- Formare il Personale
- Informare le Autorità in caso di violazione dei dati

Adottando un approccio basato sull'**analisi dei processi**, proponiamo progetti di consulenza personalizzati che prevedono:

- Analisi dei documenti già disponibili (se presenti) afferenti al trattamento di informazioni personali e all'infrastruttura ICT;
- Interviste ai responsabili degli uffici normalmente coinvolti col trattamento di dati personali per individuare i processi e i trattamenti svolti dalla struttura;
- Formalizzazione delle informazioni detenute, delle finalità e del consenso espresso al trattamento;
- Intervista con il responsabile ICT per l'analisi puntuale dell'infrastruttura informatica necessaria a gestire i trattamenti;
- Approfondimento sull'approccio aziendale alla sicurezza dei dati (Cyber Security);
- Analisi dell'adeguatezza dei contratti con clienti e fornitori coinvolti nei processi e nell'infrastruttura informatica;
- Analisi dei rischi rilevati;
- Redazione del Registro dei Trattamenti e degli allegati operativi in conformità a quanto richiesto dal GDPR.
- Informazione e formazione ai Responsabili e agli Incaricati.