GDPR 2016/679

Il GDPR (General Data Protection Regulation), entrato in vigore nell'aprile 2016 a seguito della sua pubblicazione nella Gazzetta ufficiale dell'Unione Europea, si applica con decorrenza maggio 2018 ed è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri. Il regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

GENERAL DATA PROTECTION REGULATION 2016/679

Il **GDPR 2016/679 protegge i diritti e le libertà fondamentali delle persone fisiche**, in particolare il diritto alla protezione dei dati personali.

Cosa si intende per dato personale? Con "**dati personali**" si intende **qualsiasi informazione riguardante una persona fisica, identificata o identificabile attraverso informazioni** quali il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

La norma si applica indipendentemente dal fatto che il trattamento sia effettuato o meno in territorio UE: ciò significa che riguarda anche i titolari del trattamento non stabiliti nell'UE, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

S**oggetti coinvolti**:

- **la persona fisica o titolare del dato**
- **il titolare del trattamento**
- **il responsabile del trattamento**
- **il responsabile della protezione del dato o Data Protection Officer (DPO)**
- **il Garante per la protezione dei dati**
- **la Commissione Europea per la protezione dei dati o European Data Protection Board (EDPB).**

La persona fisica diventa il soggetto interessato, che con il Regolamento acquisisce una serie di diritti, quali:

- **violazione dei dati**: notifica all'Autorità di Controllo e all'interessato in caso di violazione senza ingiustificato ritardo
- **diritto all'oblio**: diritto dell'interessato alla cancellazione dei dati personali
- **diritto alla portabilità**: diritto dell'interessato a trasferire i propri dati personali
- **diritto di accesso**: diritto dell'interessato a richiedere ed ottenere i propri dati personali e informazioni sui dati
- **diritto di opposizione**: diritto dell'interessato a chiedere il termine e la revoca del trattamento
- **diritto di limitazione:** diritto dell'interessato a chiedere la limitazione del trattamento
- **diritto di rettifica:** diritto dell'interessato a modificare i propri dati personali.

Il GDPR pone in evidenza una serie di punti di fondamentale importanza, quali:

- personal data
- trasferimento dei dati all'estero
- data portability
- consent
- privacy impact assessment
- privacy by default e privacy by design
- data protection officer
- data breach notification
- diritto alla cancellazione dei dati "diritto all'oblio"
- sicurezza dei dati personali.

I **principali passi**, che le aziende devono compiere, per ottemperare correttamente alle disposizioni del GDPR possono essere riassunti come segue:

1. **verifica di cosa si è fatto** e cosa si sta facendo (assessment con analisi cd. "as is")
2. **risk assessment e PIA** (valutazione d'impatto privacy, analisi dei rischi, classificazione dei dati etc)
3. assessment e **gap analysis**
4. **piano di remediation**
5. **nomine** ed incarichi dei soggetti coinvolti (es. Titolare, Responsabile del trattamento, Autorizzati, Responsabile della protezione dei dati/DPO se previsto etc.)
6. informazione/**formazione** del personale coinvolto
7. **aggiornamento periodico** del sistema.

Il titolare che non dovesse adempiere a quanto stabilito dal GDPR potrà incorrere in possibili sanzioni amministrative (max 20.000.000 € per le imprese, fino al 4 % del fatturato mondiale totale annuo, se superiore), civili e penali.

RINA, offre alle organizzazioni servizi differenti, in relazione al contesto aziendale e al settore di appartenenza:

- **gap analysis sul GDPR**
- **certificazione delle figure professionali rispetto alla norma UNI 11697**
- **formazione**
- **certificazioni del settore IT secondo le norme ISO 27001, ISO 20000 e ISO 22301** etc (come strumenti a supporto della sicurezza delle informazioni e protezione dei dati).

RINA Services
Via Corsica, 12
16128 Genova - Italy

T. +39 010 53851
info@rina.org

rina.org

Certification
T. +39 010 5385703
certification@rina.org