Regolamento UE 2016/679 in materia di protezione dei dati personali

Entrata in vigore

Pubblicazione nella Gazzetta Ufficiale dell'Unione Europea n. 119/2016: **4 Maggio 2016**.
Entrata in vigore: **25 Maggio 2016**.
Applicabilità in tutti i Paesi della UE: **25 Maggio 2018**.
Il Regolamento è **immediatamente applicabile** senza necessità di recepimento.
Per quanto riguarda l'Italia, il Regolamento sostituisce (non integralmente) il D. Lgs. n. 196/2003 *Codice in materia di Protezione dei dati personali* (c.d. Codice Privacy) in vigore dal 1 Gennaio 2004 ma è **necessario comunque un coordinamento normativo** (Il Garante privacy ha in corso una ricognizione normativa per verificare quali parti del Codice Privacy e quali provvedimenti generali del Garante sopravvivranno alla riforma).

TELEMATICA E SERVIZI

I principali obblighi del Regolamento UE 2016/679

•La principale novità è costituita dall' **"Accountability" (o di Responsabilizzazione del Titolare del trattamento)**: spetta autonomamente al Titolare del trattamento, previa valutazione dei rischi che incombono sui dati trattati, mettere in atto misure adeguate ed efficaci per garantire ed essere in grado di dimostrare la conformità dei trattamenti al presente regolamento, **compresa l'efficacia delle misure adottate**

•vengono dati dei **nuovi criteri per la redazione delle informative** e viene dato più potere ai soggetti interessati (accountability, diritto alla rettifica, diritto alla limitazione del trattamento, diritto all'oblio)

•sono state introdotte **nuove regole per la designazione dei responsabili del trattamento**

•è stato introdotto il concetto di **contitolarità dei dati** e stabilite le regole che la disciplinano

TELEMATICA E SERVIZI SRL
Via San Tommaso D'Aquino, 116 – 00136 Roma Tel. 06.39754455 Fax 06.39749567
P.iva e C.F. 12535361005

TELEMATICA E SERVIZI

I principali obblighi del Regolamento UE 2016/679

•un'altra novità è costituita dal **"registro dei trattamenti"** (art. 30), che contiene l'analisi di tutti i processi aziendali che comportano un trattamento dei dati personali. Si tratta di una misura obbligatoria nel caso in cui vengano effettuati trattamenti di dati sensibili o giudiziari che presentino un rischio per i diritti e le libertà dell'interessato

•**valutazione d'impatto sulla protezione dei dati** – **DPIA** (art. 35), mirata all'analisi e alla gestione di tutti i trattamenti che presentano un rischio elevato per i diritti e le libertà dell'interessato

•**notificazione al garante delle violazioni** che comportino un rischio elevato per i diritti e le libertà degli interessati (dati genetici, dati biometrici, profilazione, geolocalizzazione, ecc.)

•designazione **del Responsabile della protezione dei dati personali (Privacy Officer)**

TELEMATICA E SERVIZI

Il Responsabile della protezione dei dati (Data Protection Officer)

La designazione del DPO è obbligatoria (da parte del Titolare o del Responsabile del trattamento) solo se:

1. il trattamento **è effettuato da un'autorità pubblica o da un organismo pubblico**, eccettuate le autorità giurisdizionali;
2. le attività **principali** del Titolare del trattamento o del Responsabile del trattamento consistono in **trattamenti che,** per natura, ambito di applicazione e/o finalità, **richiedono il monitoraggio regolare e sistematico degli interessati su larga scala**;
3. le attività **principali** del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, **su larga scala**, di categorie particolari di dati di cui all'art. 9 o 10 del Regolamento (dati che rivelino l'origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, biometrici, dati relativi alla salute o alla vita sessuale o orientamento sessuale, o dati relativi a condanne penali e a reati).

Ai sensi delle disposizioni dell'art. 37 del Regolamento deve essere comunicato il nominativo del DPO al GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, mediante l'apposita procedura telematica.

Il DPO va designato in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i propri compiti.

Sanzioni

•**amministrative**: Il regolamento UE 2016/679 prevede sanzioni amministrative molto onerose (fino a 20 milioni di Euro o, se superiore, fino al 4% del fatturato mondiale annuo precedente) per ciascuna inosservanza delle disposizioni in esso contenute. Sanzioni minori sono al momento in via di definizione da parte del Garante per la protezione dei dati personali. Esse saranno con ogni probabilità di molto superiori a quelle (già ingenti) previste dal D.Lgs 196/2003.

•**penali**: le sanzioni penali nel caso di inosservanza delle disposizione del Regolamento Ue 2016/679 saranno stabilite dal Garante per la protezione dei dati personali a partire dal 25 Maggio 2018; si precisa che a queste si aggiungono gli illeciti penali previsti già nel caso in cui non vengano osservati tutti i Provvedimenti finora emanati dal Garante per la protezione dei dati personali. È altresì obbligatorio attenersi alle linee guida del gruppo di lavoro europeo WP29.

SERVIZI OFFERTI

Il nostro team di Consulenti è in grado di supportare la Vostra Azienda negli interventi formativi ed in tutti gli obblighi previsti dal nuovo Regolamento.
Si riporta di seguito una breve sintesi delle modalità di erogazione dei servizi di consulenza.

Modalità di erogazione dei servizi

La prima fase del servizio prevede la pianificazione e l'esecuzione di un check-up circa l'impatto derivante dall'applicazione del nuovo Regolamento UE in materia di data protection n. 679/2016 (GDPR-General Data Protection Regulation) sulla Azienda.
All'esito del check-up il Cliente sarà seguito e assistito sull'implementazione e aggiornamento del sistema di tutela dei dati in base alle disposizioni del nuovo Regolamento in relazione a:

- Rapporti con responsabili esterni
- Rapporti con titolari del trattamento
- Nuove regole su informative e consensi
- Privacy by design
- Privacy by default
- Registro delle attività di trattamento
- Data breaches (notifiche)
- DPIA -Data Protection Impact Assessment e la sicurezza dei dati
- DPO- Data Protection Officer
- Diritto alla cancellazione ("diritto all'oblio")
- Diritto alla portabilità dei dati
- Formazione e istruzione agli "incaricati«, Responsabili, ecc.

TELEMATICA E SERVIZI

SERVIZI OFFERTI

1. Check presso la sede del Cliente per la verifica della documentazione relativa alla tutela dei dati personali (privacy) ed all'applicazione delle misure e procedure di tutela (con redazione relazione finale)

2. Consulenza sull'adeguamento al General Data Protection Regulation (Regolamento UE 2016/679)

3. Consulenza ed assistenza annuale (compresa pianificazione di audit)

4. Assunzione dell'incarico di DPO

5. Formazione, presso la sede del clienti, della durata massima di 4 ore per gli incaricati al trattamento

6. Formazione per DPO interno (percorsi formativi da 8 ore a 80 ore)

7. Formazione sul Regolamento UE 2016/679 in materia di protezione dei dati personali (percorsi formativi da 4 e 8 ore)

TeS