NOVACONSULT
COMPLIANCE | CONSULENZE | SELEZIONE

PRIVACY
PROTEZIONE DEI DATI PERSONALI

Nuovo Regolamento Europeo 2016/679
del 27 aprile 2016

NC TEAM SRL - Via Gaetano Strambio n. 5 - 20133 Milano (MI)
Tel. 02.57408940 - Fax 02.99989424 - C.F. e P. IVA 08671990961
Capitale Sociale € 25.000,00 - REA: MI-2041984 - ncteam@pec.it

PREMESSA

Il 24 maggio 2016 è entrato in vigore il nuovo regolamento Europeo (UE) 2016/679 in materia di protezione dei dati personali. Il Regolamento è immediatamente applicabile in tutti gli Stati membri, è uguale in tutta Europa e sostituisce la precedente normativa, D.L. 196/2003, il cosiddetto "Codice Privacy".

Il Nuovo Regolamento introduce regole più chiare in materia di **informativa** e **consenso**, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali (*Data Breach)*.

Per le imprese il Regolamento europeo introduce nuovi **obblighi**:

- ✓ la predisposizione di un "**Registro dei trattamenti**" e del suo aggiornamento;
- ✓ un documento preventivo di verifica della protezione dei dati trattati (**DPIA**);
- ✓ una **valutazione d'impatto** contenente:
  - l'identificazione dei rischi possibili alla privacy nel normale svolgimento delle attività aziendali;
  - le possibili soluzioni per ridurre i rischi di violazione dei dati;
- ✓ **obbligo di notifica** in caso di perdita di dati, violazioni e hackeraggio;
- ✓ nuova informativa del trattamento e consenso.

PRINCIPALI NUOVI OBBLIGHI

- L'allestimento e tenuta del **registro dei trattamenti**
- Predisporre il documento di verifica della protezione del trattamento fin dalla progettazione (privacy by design, privacy by default)
- Una **valutazione d'impatto** sulla protezione dei dati, applicabile a trattamenti selezionati
- L'obbligo di notifica in caso di violazione o perdita dei dati personali o sensibili - **Data Breach**
- Nomina del **Data Protection Officer (DPO)** – Responsabile della Protezione dei dati
- Formazione del personale(tutti coloro che trattano i dati in azienda, a tutti i livelli)
- Limiti al trasferimento al di fuori dell'UE: è vietato il trasferimento di dati personali verso Paesi al di fuori dell'Unione europea che non rispondono agli standard europei
- Obbligo di trasparenza e rendicontazione - **Accountability**

LE NUOVE FIGURE

(Art. 4 GDPR)

- **RESPONSABILE DEL TRATTAMENTO**: La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare del trattamento.

- **TITOLARE DEL TRATTAMENTO**: La persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

- **INCARICATO**: Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

- **INTERESSATO**: Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Per alcune tipologie di dati/trattamenti viene introdotta la figura del **DPO** (**Data Protection Officer**) incaricato di controllare la correttezza della gestione dei trattamenti da parte della società.

Il DPO, in possesso di adeguate conoscenze e competenze, potrà essere un dipendente o un consulente e dovrà avere delle specifiche abilitazioni (art. 37 GDPR). In particolare dovrà:

- Possedere un'adeguata conoscenza della normativa e della prassi di gestione dei dati personali;
- Adempiere alle sue funzioni in piena indipendenza ed in assenza di conflitti di interesse.

Il **DPO** è previsto **obbligatoriamente** nei seguenti casi:

- Amministrazioni ed enti pubblici
- Tutti i soggetti che effettuano trattamenti "di massa o su larga scala"
- Tutti i soggetti che svolgono il trattamento di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici

La lista completa dagli enti e dei trattamenti che dovranno dotarsi del DPO è consultabile sul documento UE WP29.

POSSIBILI SANZIONI

L'Autorità garante ha il potere di commisurare una sanzione:

- fino a **€ 20 milioni**;
- fino al **4%** del fatturato mondiale totale annuo.

Oltre a questo occorre considerare:

- **RESPONSABILITÀ CIVILE**
  - Richiesta di risarcimento danni da parte degli interessati
  - Azioni collettive (*class action*)
- **RESPONSABILITÀ AMMINISTRATIVA**
  - Sanzioni amministrative
  - Ispezioni a sorpresa (Guardia di finanza)
  - Blocco del trattamento dei dati in violazione di legge
- **RESPONSABILITÀ PENALE**
  - Sanzioni penali nei confronti degli organi apicali
  - Responsabilità amministrativa degli enti (D. Lgs. 231/01)
- **DANNO REPUTAZIONALE**
  - Attenzione della stampa
  - Perdita di fiducia dei consumatori
  - Perdita di fiducia dei fornitori

LA NOSTRA PROPOSTA

La nostra Società, mediante sopralluoghi ed interviste con i referenti aziendali, si propone di predisporre le misure organizzative e procedurali per la gestione dei dati, conformi ai contenuti del Regolamento UE 2016/679.

In particolare, l'attività di consulenza ha l'obiettivo di:

- Analizzare le procedure di sicurezza e le modalità di archiviazione dei dati applicate dalla Società, valutandone la loro adeguatezza al Regolamento UE [**Check procedure e attrezzature informatiche**]
- Identificazione/nomina delle figure previste dalla normativa (titolare, responsabile, incaricati, lettere di incarico, deleghe) [**Check deleghe**]
- **Informativa del trattamento e consenso**
- Predisposizione di procedure per l'archiviazione, gestione, protezione dei dati e autenticazione degli accessi
- Allestimento e tenuta del "**Registro dei trattamenti**" e del "Documento di verifica della protezione dei dati trattati" [DPIA – Data Protection Impact Assessment]
- **Nomina del DPO – Data Protection Officer**
- Addestramento e formazione del personale, addetti e incaricati
- Check trattamento dei dati fuori dall'UE
- Procedure per la gestione delle violazioni (**Data Breach**)