

STUDIO LEGALE ASSOCIATO
MARTINEZ & NOVEBACI

20129 MILANO
Via Archimede, 56
Tel. 0270002339
Fax 02740707



ASSOCIAZIONE ITALIANA AVVOCATI D'IMPRESA
e-mail: studio.milano@martinez-novebaci.it
www.martinez-novebaci.it
Sede di Milano

10129 TORINO
Via Caboto, 44
Tel. 01119700759
Fax 01119700760

33139 MIAMI BEACH
1680 Michigan Avenue
Tel. 001.3057772274
Fax 001.3057772278

EC4Y ODB LONDRA
3-7 Temple Avenue
Tel. +44 (0) 20 75838625
Fax +44 (0) 20 75838629

GDPR EU 679/2016

Regolamento Europeo in materia di Trattamento dei Dati

Il 25 Maggio 2016 è entrato in vigore il Regolamento Europeo Privacy (GDPR 679/2016) e dal prossimo 25 maggio 2018 sarà effettivamente applicabile a tutte le realtà aziendali e professionali.

La costante evoluzione delle nuove tecnologie e il costante ricorso a database ha imposto all'Unione Europea l'adozione di regole unitarie per tutti i trattamenti di dati realizzati nel territorio degli stati membri dell'Unione. Il GDPR – acronimo di General Data Protection Regulation - ha infatti l'obiettivo di fortificare i diritti delle persone fisiche e unificare la Normativa in merito alla protezione dei dati personali all'interno di tutta l'Unione Europea, sostituendo le diverse leggi nazionali presenti nei Paesi Membri.

Il Regolamento abroga, dunque, la Direttiva 95/46/CE, recepita dall'attuale D.lgs. 196/2003 (c.d. Codice Privacy) e introduce i nuovi Principi su cui fondare ogni tipologia di trattamento dati:

- **LICEITA', CORRETTEZZA E TRASPARENZA**
- **LIMITAZIONE DELLE FINALITA'** che dovranno essere determinate, esplicite e legittime
- **MINIMIZZAZIONE DEI DATI** raccolti, limitati ai soli dati effettivamente necessari, adeguati, pertinenti
- **ESATTEZZA DEI DATI**
- **LIMITAZIONE DELLA CONSERVAZIONE** per un periodo temporale limitato al conseguimento delle finalità
- **INTEGRITA' E RISERVATEZZA** al fine di garantire un'adeguata sicurezza dei dati e protezione da possibili Data Breach (violazione dei dati).
- **RESPONSABILIZZAZIONE** in quanto il Titolare è tenuto a comprovare il rispetto di tali principi.

Il nuovo GDPR vede profondamente rinnovato il concetto di privacy ed introdotto quello di data protection by design e data protection by default – ovvero protezione dei dati fin dalla

progettazione – con ciò imponendo alle aziende il ripensamento dei singoli processi aziendali e la creazione di uno specifico modello di organizzazione che debba prevedere, almeno in questa fase di adeguamento, alcuni step imprescindibili:

- **MAPPATURA DEI TRATTAMENTI** e di tutti i dati raccolti;
- **DEFINIZIONE DI MISURE DI SICUREZZA ADEGUATE E IDONEE PROCEDURE ORGANIZZATIVE**
- **INDIVIDUAZIONE DI RUOLI, COMPITI E RESPONSABILITÀ;**
- **DOCUMENTAZIONE DELLA CONFORMITÀ**

Proprio in tema di riorganizzazione aziendale e definizione di ruoli, il GDPR introduce delle figure chiave nel nuovo panorama Privacy distinguendo tra Titolare, DPO, responsabili e incaricati del trattamento.

Il **Titolare del trattamento** rimane il soggetto incaricato di implementare l'adozione di opportune misure di sicurezza e di dimostrarne la conformità al Regolamento in caso di controlli, gravando su di esso sia l'eventuale risarcimento dei danni nei confronti del soggetto interessato sia le sanzioni da parte delle autorità di controllo.

Ad affiancare la figura del Titolare, con una funzione di informazione, consiglio e controllo interno, il GDPR introduce a livello europeo il **Data Protection Officer (DPO)** il cui compito è quello di garantire la conformità dell'organizzazione aziendale ai requisiti stabiliti dal Regolamento, agendo in modo indipendente e ponendosi quale figura garante tanto degli interessi del Titolare che dell'utente i cui dati vengono raccolti. La nomina del DPO è obbligatoria se l'azienda *a)* è un organismo pubblico; *b)* esercita come attività principale un trattamento che comporta la sorveglianza regolare e sistematica di soggetti su larga scala; *c)* esercita come attività principale un trattamento di dati particolari o giudiziari su larga scala.

Il Titolare potrà nominare dei responsabili e degli incaricati del trattamento, esterni o interni all'azienda, i quali hanno accesso ai dati per ragioni aziendali, tecniche o commerciali ma sui quali non ricadono le medesime responsabilità previste dal Regolamento per il Titolare.

In tema di responsabilità, il GDPR chiarisce che il rispetto delle norme in materia di protezione dei dati fa parte della **RESPONSABILITÀ D'IMPRESA DEL TITOLARE DEL TRATTAMENTO** (e non del DPO).

Se dunque il DPO potrebbe rispondere solo a titolo di responsabilità professionale, il Titolare del trattamento risponde direttamente e interamente in tutte le ipotesi di inosservanza e, anche in caso di inadempimenti derivanti da colpa o dolo del DPO, il Titolare o il Responsabile potranno solo avanzare pretese risarcitorie a titolo di responsabilità contrattuale.

Le sanzioni che, in caso di non conformità, graverebbero sul Titolare potranno raggiungere fino a **20 MILIONI DI EURO** per i privati e per le imprese non facenti parte di gruppi e fino al **4% DEL FATTURATO CONSOLIDATO** per i gruppi societari.

La nuova normativa obbliga, dunque, ad un approccio nuovo, multidisciplinare e globale che coinvolge tutte le tipologie di trattamento e tutti i dati personali raccolti, che siano quelli dei clienti, dei fornitori o dei dipendenti e nessuna società, ditta individuale o studio professionale può dirsi al sicuro rispetto agli adempimenti imposti dal GDPR, indipendentemente dalla grandezza o dal numero di collaboratori.

L'attività dello Studio Legale Martinez & Novebaci

Lo Studio è in grado di fornire assistenza e consulenza a 360° sui seguenti temi:

- analisi dello stato di conformità dell'azienda;
- procedure e istruzioni per l'adeguamento al GDPR;
- redazione di Informativa Privacy e verifica delle procedure di consenso;
- classificazione di dati e trattamenti;
- incarichi e nomine Privacy (compresa la nomina del DPO);
- notificazioni al Garante Privacy;
- Data Protection Impact Assessment (DPIA), laddove necessario.

L'intervento da parte dello Studio si potrà articolare in **due fasi**, di cui la prima fase volta alla valutazione generale della situazione della Società, alla identificazione dello stato di conformità al GDPR 2016/679, attraverso un'analisi di persone, processi, organizzazione, tecnologie e strumenti, come di seguito elencato:

- i) ricezione di tutta la documentazione fornita dalla Società in grado di rilevare gli aspetti dell'operatività in termini di privacy, quali il contesto aziendale (dimensione, numero addetti, organigramma), regolamenti e procedure già in atto in ambito normativo privacy, le attività dei vari uffici che comportano trattamenti dati personali, le politiche poste in essere dall'Ufficio Privacy (se preposto), le attività di formazione in materia privacy, le infrastrutture ICT ed il grado di supporto che quest'ultime forniscono alla privacy;
- ii) analisi della documentazione e della risultanze emerse dagli incontri e dai colloqui avuti con la Società;
- iii) redazione di un breve report, il quale contenga la descrizione della situazione attuale della Società, un'analisi della conformità della Società e dei suoi processi al GDPR, un elenco delle soluzioni e delle misure da adottare per essere conformi al GDPR;
- iv) consegna di un manuale operativo che potrà essere utile alla Società nello svolgimento delle attività di utilizzo e trattamento dati;
- v) accesso presso la Società, da parte di un avvocato dello Studio, per consulto e una verifica finale.

La seconda fase, meramente facoltativa seppur fortemente consigliata, volge invece a prestare assistenza telematica continuativa nel periodo successivo alla prima fase in tutte le tematiche e le problematiche afferenti la privacy, con supporto costante nei vari aggiornamenti della normativa e delle linee guida fornite dal Garante.

Qualora il Cliente ne faccia espressa richiesta, lo Studio offre altresì, quale servizio aggiuntivo, la possibilità di mettere a disposizione un proprio professionista di fiducia che rivesta, per conto dell'azienda, il ruolo del Data Protection Officer.