STUDIO ASSOCIATO
BOLLA
BERGERO
BIANCO
Corporate
Tax
Legal
consultancy

NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY (GDPR Reg. UE n. 679/2016): COME CAMBIA L'APPROCCIO SULLA DATA PROTECTION

Il 24 maggio 2016 ha avuto inizio una vera e propria rivoluzione, che troverà il suo pieno compimento il prossimo 25 maggio 2018.

L'Unione Europea ha concesso due anni di tempo per permettere ad oltre l'80% delle aziende italiane (ed al 58% di quelle europee) di adeguarsi al nuovo **Regolamento UE n. 2016/679** (GDPR) **sulla protezione dei dati personali**. Infatti, le aziende italiane ed europee non conoscono ancora il GDPR (e neppure risultano del tutto allineate alle prescrizioni del Codice della Privacy, a tutt'oggi in vigore), ma soprattutto non hanno ancora percepito la gravità del rischio sanzionatorio da cui saranno colpite, in caso di scorretto utilizzo dei dati e delle informazioni riguardanti i propri clienti ed utenti.

La corretta circolazione dei dati e l'adeguatezza dell'organizzazione societaria alle regole nazionali ed europee devono diventare una priorità per ogni soggetto economico, che utilizzi dati oltre lo spazio fisico / geografico suo proprio, disponendone e condividendoli in tempo reale. La Privacy deve essere considerata come un *asset* da valorizzare da parte di ogni azienda, soprattutto se utilizza mezzi di profilazione e di *marketing* sui dati dei propri clienti, da cui intende, appunto, ricavarne "profitto". Le attività di *compliance* e di *governance* devono riguardare tutte le aziende, grandi e piccole, quale che sia il business ed il settore merceologico in cui si muovono.

Le novità più rilevanti riguardano l'istituzione della figura del ***Data protection officer*** ("DPO"), il ***data breach***, il riconoscimento normativo del **diritto all'oblio** e le **misure di sicurezza** sui dati. Più in generale, il GDPR ha ripensato le basi della normativa *privacy* fondandole sul **principio di adeguatezza** delle misure da adottare a garanzia dei dati e sulla **responsabilizzazione** (*accountability*) dei soggetti che effettuano il trattamento.

Il GDPR è applicabile a tutte le imprese presenti negli Stati membri - anche se situate al di fuori dell'UE - che trattino dati personali nel territorio dell'Unione. Per dato personale si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente. Le **sanzioni** comminabili ai trasgressori ammonteranno **fino a 20 milioni di Euro** o, per le imprese che superano tale soglia di **fatturato mondiale annuo**, **fino al 4%** dello stesso, registrato nell'esercizio precedente.

Di seguito, una breve panoramica delle maggiori novità del GDPR.

Data Protection Officer

Il GDPR prevede l'obbligo di nomina di un Responsabile per la protezione dei dati (DPO) all'interno di tutte le **autorità** e gli **enti pubblici**, nonché in tutte quelle **società** i cui Titolari o Responsabili svolgano come attività principa-

GENOVA
Via XX settembre 33/7
16121 GENOVA
Tel +39 010 5705003
Fax +39 010 566758

MILANO
Viale Premuda 46
20129 MILANO
Tel +39 02 7788631
Fax +39 02 778863258

TORINO
Corso G. Matteotti 17
10121 TORINO
Tel +39 011 4542526

SAVONA
Via Paleocapa 19/3
17100 SAVONA
Tel +39 019 814255
Fax +39 010 566758

Corporate
Tax
Legal
consultancy

le il trattamento di dati con monitoraggio regolare e sistematico, su larga scala, o la gestione, sempre su larga scala, di speciali categorie di dati.

Il DPO dovrà fornire la propria consulenza e professionalità al fine di **costruire un sistema organizzato di gestione dei dati personali**, svolgendo attività di verifica e di vigilanza.

L'adozione su base volontaria dei DPO da parte di Titolari e Responsabili del trattamento è consentita e, anzi, incoraggiata a livello europeo. La nomina di un tale soggetto, infatti, può facilitare sensibilmente gli oneri di *compliance* e costituire un vantaggio competitivo per l'esercizio dell'impresa.

Registro dei Trattamenti

Il Registro dei Trattamenti è un **documento che censisce le caratteristiche principali dell'attività del Titolare del trattamento e del Responsabile del trattamento**. La funzione del Registro è prevalentemente descrittiva e il suo contenuto deve corrispondere alla realtà dei fatti

Sono obbligati a tenere ed aggiornare il Registro tutti i Titolari e Responsabili del trattamento, ad eccezione di imprese e/o organizzazioni con **meno di 250 dipendenti**

Sono comunque obbligate anche le imprese e le organizzazioni sotto la soglia dei 250 dipendenti qualora:

- ✓ il trattamento effettuato possa presentare un rischio per i diritti e le libertà degli Interessati,
- ✓ il trattamento non sia occasionale,
- ✓ vengano trattate categorie particolari di dati personali quali, a titolo di esempio, dati che rivelino l'origine razziale o etnica, le opinioni politiche, dati genetici, biometrici o dati relativi alla salute o alla vita sessuale

Data breach

Il GDPR prevede obblighi e rimedi in capo al Titolare ed al Responsabile del trattamento in caso di violazione dei dati personali. Il *Data Breach* consiste in **qualsiasi tipo di attività che abbia come conseguenza** una **perdita del controllo** dei dati personali, **discriminazione**, **furto d'identità**, **perdite finanziarie**, **decifratura non autorizzata** della pseudonimizzazione, **perdita reputazionale**, **perdita di riservatezza** dei dati protetti da segreto professionale, ogni altro **danno economico o sociale** al *data subject*.

Il Titolare del trattamento che scopre una violazione deve procedere alla **notifica all'Autorità di controllo competente** (in Italia, il Garante Privacy). La **notifica** deve essere effettuata **entro 72 ore dalla conoscenza** del fatto, se possibile, oppure **oltre 72 ore**, con specificazione dei **motivi del ritardo**. La

Corporate
Tax
Legal
consultancy

notifica è obbligatoria, salvo il caso in cui "*sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*".

Sicurezza dei dati

Il GDPR si focalizza sulla **prevenzione dei rischi sui dati**. Il Titolare del trattamento deve provvedere all'adozione di misure di sicurezza **adeguate**, che possono essere sia **tecniche** che **organizzative**, come la **pseudonimizzazione** e **cifratura** dei dati personali; l'assicurazione su base permanente della riservatezza, integrità, disponibilità e resilienza di sistemi e servizi di trattamento; capacità di **ripristino tempestivo** di disponibilità ed accesso ai dati in caso di incidente; adozione di una **procedura per testare**, verificare e valutare **l'efficacia delle misure** tecniche e organizzative.

Diritto all'oblio

Il GDPR ha ufficialmente introdotto il **diritto all'oblio**, ossia il diritto **di ogni individuo alla cancellazione dei propri dati, al fine di non essere più ricordato per fatti che lo riguardino e che in passato siano stati oggetto di cronaca**. Tali richieste possono essere fatte valere nei confronti dei gestori dei motori di ricerca sulla rete, al fine di ottenere la rimozione dai propri risultati di ricerca *web* ("deindicizzazione") o di chiedere ad un altro sito *web* la cancellazione di informazioni. L'interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, e il Titolare ha l'obbligo di provvedere, qualora sussista uno dei seguenti motivi: **esaurimento delle finalità** per cui i dati sono stati raccolti o trattati; **revoca del consenso** da parte dell'interessato; **opposizione al trattamento** da parte dell'interessato; **illiceità del trattamento** dei dati da parte del Titolare; **obbligo legale** a cui è soggetto il Responsabile del trattamento. Il **Titolare** del trattamento, qualora abbia reso pubblici i dati personali e sia obbligato a cancellarli, tenuto conto della tecnologia a lui disponibile e dei costi di attuazione, **prende le misure ragionevoli per informare i Responsabili del trattamento** che stanno trattando i dati a proposito della richiesta dell'interessato di cancellare qualsiasi *link*, copia o riproduzione dei suoi dati personali.

Gli altri nuovi diritti

Diritto al Consenso Attivo

Il diritto di poter esprimere attivamente il proprio consenso dopo aver ricevuto una chiara informativa *privacy* e di poterlo in ogni momento revocare.

Diritto alla Portabilità dei Dati

Corporate
Tax
Legal
consultancy

Il diritto di poter trasferire in maniera semplice e agevole i propri dati personali da un *provider* ad un altro fornitore di servizi.

Diritto alla Trasparenza Informativa

Il diritto di ricevere un'informativa *privacy* preventiva chiara, semplice e comprensibile.

Diritto alla Profilazione Consenziente

Il diritto che le attività di profilazione non vengano effettuate in maniera automatizzata e senza il preventivo ed espresso consenso dell'interessato.

Diritto alla *Privacy* dei Minori

Il diritto a che i dati dei minorenni siano protetti in maniera più sicura e trattati solo con il preventivo consenso dei genitori (consenso legittimo del minore fissato a 16 anni, con delega da parte del GDPR ai Singoli stati membri di abbassamento della soglia fino a 13 anni). Lo schema di Decreto Legislativo in corso di approvazione prevede l'abbassamento del limite di età a 14 anni (art. 6).