AMBIENTEROSA
consulenze ambientali
Società Responsabilità Limitata
Amministratore Unico: Rosa Bertuzzi
Via Pantalini, 9
29121 - Piacenza
P. Iva 01711730331
rosabertuzzi@ambienterosa.net
PEC: ambienterosa@legalmail.it
www.ambienterosa.net

di **Avv. Rosa Bertuzzi**

NUOVI OBBLIGHI A CARICO DELLE AZIENDE SULLA PRIVACY

Il 25 maggio 2018 è il giorno in cui il nuovo Regolamento UE 2016/679 sarà direttamente applicato in tutti i Paesi dell'Unione Europea e andrà a sostituire l'attuale Codice della Privacy (Dlgs 196/2003) oggi vigente in Italia. Il Regolamento introdurrà regole più chiare e semplici in materia di informativa e consenso, puntando a garantire maggiori tutele per i cittadini in maniera omogenea in tutta l'Unione, sebbene ogni Stato possa integrare i contenuti del regolamento. In Italia questo ruolo sarà ancora gestito dal Garante della Privacy. Il regolamento diventerà immediatamente applicabile senza bisogno di essere recepito con provvedimenti nazionali; avremmo quindi un testo unico valido in tutti i paesi UE che mirerà a rendere omogeneo ed elevato il livello di protezione dei dati personali e a favorire la circolazione degli stessi all'interno dell'Unione Europea. Agli Stati Membri dell'Unione rimarrà la possibilità di introdurre ulteriori regole e condizioni.

Con l'uscita del Regolamento n. 679 non verranno aboliti i provvedimenti del nostro Garante su Videosorveglianza, Amministratori di Sistema, fidelity card, biometria e tracciamento flussi bancari. È quindi probabile che il Garante Privacy modifichi o integri alcuni provvedimenti per adeguarli alle prescrizioni del Regolamento Europeo n. 679. Il Garante Privacy italiano potrà inoltre integrare il Regolamento UE 679 per disciplinare il trattamento di dati personali effettuato per adempiere obblighi di legge italiana ed in particolari ambiti, ad esempio quello dei dati sanitari, oppure per definire in modo più dettagliato gli obblighi per le PMI (ovvero per le imprese con meno di 250 dipendenti).

Il Regolamento 679 disciplinerà esclusivamente il trattamento di dati personali relativi a persone fisiche non decedute, quindi tutti i trattamenti relativi a persone giuridiche, compresi il nome, la forma della persona giuridica ed i suoi dati di contatto.

Verranno stabiliti nuovi limiti al trattamento automatizzato dei dati personali e criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue. Entra in vigore l'obbligo di segnalazione per i casi di violazione dei dati personali (data breach).

Significativi cambiamenti riguardano l'informativa ed il consenso. L'informativa andrà resa in forma concisa, trasparente, intellegibile, facilmente accessibile e con un linguaggio semplice e chiaro; le informazioni saranno fornite per iscritto o con altri mezzi (anche in formato elettronico) e, se richiesto dall'interessato, potrà essere fornita anche oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Per quanto attiene il consenso, sarà valida qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile con la quale l'interessato accetta, con dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento. Viene esclusa ogni forma di consenso tacito oppure raccolto attraverso la presentazione di opzioni già selezionate. Il consenso potrà essere revocato in ogni momento. Il trattamento effettuato fino a quel momento dal titolare sulla base del consenso rimarrà comunque legittimo.

Verrà introdotto il cosiddetto «diritto all'oblio»: il diritto da parte di un interessato ad ottenere la cancellazione dei propri dati personali, anche on line, da parte del titolare del trattamento, qualora ricorrano alcune condizioni previste dal Regolamento: i dati saranno trattati solo sulla base del consenso; se i dati non saranno più necessari per gli scopi rispetto ai quali sono stati raccolti; se i dati sono trattati illecitamente; oppure se l'interessato si oppone legittimamente al loro trattamento. Il diritto all'oblio potrà essere limitato solo in alcuni casi specifici: per esempio, per garantire l'esercizio della libertà di espressione o il diritto alla difesa in sede giudiziaria; per tutelare un interesse generale (ad esempio, la salute pubblica); oppure quando i dati, resi anonimi, sono necessari per la ricerca storica o per finalità statistiche o scientifiche.

Il nuovo regolamento introduce la portabilità dei dati per favorire una maggiore fluidità del mercato digitale. Tra le possibilità che il regolamento permette c'è il trasferimento dei dati da un titolare del trattamento ad un altro, si potrà cambiare il provider di posta elettronica senza perdere i contatti ed i messaggi salvati, salvaguardando il diritto di essere totalmente dimenticato da chi ha raccolto i dati inizialmente.

Più garanzie per i minori: i fornitori di servizi Internet ed i social media, dovranno richiedere il consenso ai genitori o a chi esercita la potestà genitoriale per trattare i dati personali dei minori di 16 anni.

Saranno necessarie valutazioni d'impatto sulla protezione dei dati, o Privacy Impact Assessment in caso di trattamenti rischiosi e verifiche preliminari per diverse circostanze da parte del Garante. Si valicherà, peraltro, la prassi di notificazione all'autorità, con notevole semplificazione per le attività d'impresa plurinazionali.

Il Data Protection Officer, abbreviato in DPO, rappresenta una nuova figura nel panorama italiano che verrà introdotta dal nuovo Regolamento UE 679.

Con il nuovo Regolamento, imprese ed enti avranno più responsabilità, ma potranno beneficiare di semplificazioni ed in caso di inosservanza delle regole saranno previste sanzioni, anche elevate. È importante studiare tempestivamente l'impatto dell'applicazione del nuovo Regolamento sulla propria realtà lavorativa

QUALI SONO GLI OBBLIGHI NEI CONFRONTI DEI DIPENDENTI:

- **PRINCIPIO GENERALE (GDPR, Art. 5, 6, 24, 30, 32)**

  La novità principale della normativa è il **principio di accountability – Responsabilizzazione del Titolare**, basato sull'obbligo di dimostrare, documentare e personalizzare il proprio adeguamento.

- **NOMINA SOGGETTI (GDPR, Art. 26, 28, 29, 37)**

  La normativa prevede l'assegnazione di adeguati ruoli e responsabilità a **tutti i soggetti coinvolti** in operazioni di trattamento dei dati **(autorizzazioni ed istruzioni al personale interno),** nonché la richiesta di specifiche clausole di garanzia per tutti i soggetti esterni che possono accedere ai dati stessi.

  La normativa introduce la figura del **Data Protector Officer (Responsabile della protezione dei dati)**, soggetto, anche esterno, preposto a gestire e monitorare la conformità al GDPR.

- **NUOVI OBBLIGHI (GDPR, Art. 25, 33, 34)**

  Il Titolare dovrà tenere un **registro delle violazioni di dati personali** procedendo entro 72 ore, qualora la violazione possa comportare significativi rischi, a comunicarla all'Autorità di Controllo. Viene, inoltre, introdotto il principio chiave del **"privacy by default e by design"** ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche.