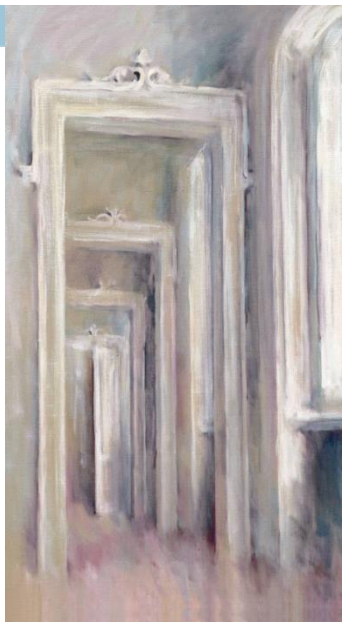
STUDIO LEGALE
PADOVAN

Client Alert
Aprile 2018



GDPR: sei pronto per adeguarti al nuovo Regolamento europeo in materia di privacy?

Il nuovo Regolamento 2016/679 sulla protezione dei dati personali. Linee guida

A partire dal maggio prossimo, la regolamentazione comunitaria apporterà rilevanti novità legislative destinate ad incidere sulla tutela legale del trattamento dei dati personali e sulla stessa organizzazione dei dati adottata dalle aziende. Di seguito, una panoramica introduttiva delle principali novità e di alcuni aspetti di carattere transnazionale.

Il Regolamento 2016/679, approvato il 27 aprile 2016 e pubblicato nella GUE il 4 maggio 2016 (il "Regolamento"), prevede un riordino sistematico della disciplina del trattamento dei dati personali. Il Regolamento sarà applicabile dal **25 maggio 2018** e, abrogando espressamente la Direttiva 95/46/CEE, sostituirà la normativa nazionale di attuazione in materia di *privacy,* fatta salva la potestà concessa agli Stati membri di regolamentare ulteriormente taluni aspetti della nuova disciplina. Per quanto riguarda l'Italia, la vigente normativa è costituita dal D. Lgs. 196/2003 ("Codice della Privacy"). Tale codice, se verrà confermato quanto espresso dal Comunicato stampa del Consiglio dei Ministri n 75 e nella Relazione Illustrativa che accompagna il testo provvisorio dello schema di decreto legislativo di armonizzazione, verrà completamente abrogato in un'ottica di semplificazione legislativa.

Di seguito, una breve rassegna sulle principali novità introdotte dal Regolamento:

- ***Regolamento e leggi nazionali.*** Il Regolamento ha lo scopo di unificare la normativa in tutta l'UE. Nonostante tale dichiarato obiettivo, esso consente agli Stati membri di mantenere o introdurre regole specifiche per determinati aspetti.
- ***Ambito di applicazione***: E' circoscritto ai **dati relativi alle persone fisiche** (con esclusione dei dati relativi alle persone giuridiche).

Per maggiori informazioni, contattare:

Avv. Marco Padovan
mpadovan@studiopadovan.com

Avv. Josè Cienfuegos
jcienfuegosi@studiopadovan.com

Avv. Tobia Cantelmo
tcantelmo@studiopadovan.com

Dott.ssa Giulia Levi
glevi@studiopadovan.com

- Il Regolamento risulta applicabile "indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione" anche a Titolari e Responsabili (le definizioni coincidono sostanzialmente con quelle del Codice della Privacy), non stabiliti nel territorio dell'Unione, qualora: (i) trattino dati personali di persone fisiche che si trovano nell'UE quando il trattamento è in relazione a offerte di beni e servizi, indipendentemente dal fatto che sia richiesto o meno un pagamento; o (ii) effettuino attività di monitoraggio sul comportamento di persone fisiche che si trovano nell'UE, qualora tale comportamento avvenga in territorio UE. Il Regolamento individua poi un'unica autorità di controllo (il Garante per la Protezione dei Dati personali, nel caso dell'Italia) in caso di **trattamento di dati che coinvolga in modo sostanziale soggetti di Stati membri diversi**: quella del **luogo dello stabilimento principale e/o unico del Titolare o del Responsabile ("Autorità Capofila")**, qualora questi ultimi effettuino trattamenti transfrontalieri.
- ***Accountability e Minimizzazione dei dati***: Il Titolare dovrà dimostrare l'adozione di politiche e misure adeguate in conformità al Regolamento. A corollario, sono stabiliti, tra gli altri, i principi di ***privacy by design*** - in forza del quale Il Titolare deve adottare adeguate misure tecniche e organizzative di tutela sin dalla progettazione del trattamento - e di ***privacy by default*** - ovvero l'obbligo di adottare misure e tecniche che, già dall' impostazione iniziale ("by default") garantiscano l'utilizzo dei soli dati personali necessari per ogni specifica finalità di trattamento.
- ***Data Protection Impact Assessment.*** Qualora concorrano le circostanze richiamate dall'art. 35 GDPR, il Titolare è tenuto ad effettuare una valutazione d'impatto sulla protezione dei dati che dovrà contenere: (i) una descrizione dei trattamenti previsti e delle finalità del trattamento; (ii) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; (iii) una valutazione per i rischi per i diritti e le libertà degli interessati e le misure previste per affrontare i rischi.
- ***Registri delle attività di trattamento***. Il Responsabile e il Titolare devono tenere un registro delle attività di trattamento in forma scritta, anche in formato elettronico, con le caratteristiche specificate dall'art. 30 GDPR.

- ***Diritto all'oblio***. Viene inserita una regolamentazione legale del c.d. "diritto all'oblio", elaborato dalla giurisprudenza e dai regolatori nel contenuto e nei limiti. L'interessato potrà pretendere la cancellazione dei dati pubblicati e il Titolare dovrà adottare misure ragionevoli, anche tecniche, per informare della richiesta di cancellazione i Titolari che stanno trattando i dati personali. I limiti al diritto all'oblio sono sostanzialmente riferibili ad esigenze di interesse pubblico e/o di libertà di espressione.
- ***Responsabile della protezione dei dati.*** Il Titolare e il Responsabile devono designare un **responsabile della protezione dei dati** (c.d. ***data protection officer***, di seguito **"DPO"**, da non confondere con il Responsabile) quando: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, escluse le autorità giurisdizionali nell'esercizio delle loro funzioni, oppure b) le attività principali del Titolare o del Responsabile consistono in trattamenti che, per loro natura, ambito e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala, oppure c) le attività principali del Titolare o del Responsabile consistono nel trattamento, **su larga scala,** di dati sensibili o di dati relativi a condanne penali e a reati.
- ***Portabilità dei dati.*** L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano e ha il diritto di trasmettere tali dati a un altro Titolare, senza impedimenti da parte del Titolare cui li ha inizialmente forniti.
- ***Data Breach.*** Obbligo di notifica per ogni Data Breach, verso le autorità competenti, entro 72 ore dalla loro scoperta.
- ***Sanzioni amministrative***. L'autorità di controllo ha il potere di imporre sanzioni amministrative per un importo pecuniario massimo predeterminato, tenendo conto di determinati indici (ad esempio, (i) la natura, la gravità e la durata della violazione, (ii) il carattere doloso o colposo della stessa, (ii) le misure adottate dal Titolare). **Le sanzioni alle imprese possono essere inflitte fino al 4% del fatturato mondiale annuo del trasgressore con un limite massimo di 20 milioni di Euro.** Gli Stati membri dovranno stabilire le ulteriori sanzioni (anche penali) assicurandone la proporzionalità e l'efficacia dissuasiva.

***

Gli enti e le società che devono affrontare il trattamento di dati personali dovranno sostenere, durante i prossimi giorni, la transizione verso un nuovo ed articolato sistema. E' ragionevole ritenere che, di tale sistema improntato all'uniformazione della normativa di settore, beneficeranno le società stabilite nei diversi Stati membri; tale uniformità della disciplina dovrebbe, infatti, consentire un risparmio in termini di consulenza specializzata e gestione della *compliance* aziendale.

Indubbiamente, le società operanti nel settore dell'IT, *dell'e-commerce*, le banche e le assicurazioni saranno interessate ad un processo di adeguamento che dovrà concludersi entro il 25 maggio 2018. Deve in ogni caso tenersi in considerazione che la nuova normativa impatterà anche sulle attività di società - non operanti negli specifici settori sopra menzionati – che comportino, comunque, il trattamento di dati personali (si pensi, ad esempio, alle operazioni di M&A oppure alla raccolta di dati di soggetti proveniente da Paesi terzi nell'ambito di attività legate all'export control).

Siamo naturalmente disponibili ad accompagnarvi in tale processo di adeguamento e ad offrirvi il supporto necessario in vista del 25 maggio 2018.