STUDIO
COLOMBO
CIPOLLA
MATTAVELLI
MARCHESI
E ASSOCIATI
COMMERCIALISTI
E AVVOCATI

Milano, 6 dicembre 2017

A tutti i Sigg.ri Clienti
Loro Sede

CIRCOLARE N. 40/2017

LA NUOVA DISCIPLINA DELLA PRICACY (REGOLAMENTO EUROPEO 2016/679) – ASPETTI GENERALI

PREMESSA

Il prossimo 25 maggio 2018 sarà efficace in tutti i Paesi della UE il Regolamento Europeo che disciplina il trattamento e protezione dei dati personali (n. 2016/679 - *General Data Protection Regulation*, in breve "**GDPR**"); tale disciplina è attualmente contenuta nel D. Lgs. n. 196/2003.
Le novità previste dal GDPR sono così numerose e significative da rivoluzionare la materia e produrre sulle imprese un fortissimo impatto dal punto di vista tecnologico e, soprattutto, sotto il profilo organizzativo e legale, obbligandole a reimpostare i processi aziendali, a riprogettare il sistema informativo, a rivedere deleghe e nomine, nonché a porre immediatamente in essere taluni adempimenti e misure per non arrivare impreparate alla data del 25 maggio 2018.
Ad oggi, mancano i provvedimenti tesi ad adeguare il quadro normativo nazionale alla disciplina di cui al GDPR che, oltretutto, suscita numerosi dubbi interpretativi. Il Garante per la protezione dei dati personali ha redatto una prima guida in cui fornisce raccomandazioni specifiche ai fini dell'applicazione di detta disciplina, specificando, però, testualmente che la guida stessa "*è soggetta ad integrazioni e modifiche alla luce dell'evoluzione della riflessione a livello nazionale ed europeo*".

SINTESI DEI PRINCIPALI MUTAMENTI

Qui di seguito si espongono in modo molto sintetico alcune delle principali novità contenute nel GDPR che più interessano le imprese.
- **Nuovi principi**: mentre nel sistema attuale l'adozione delle misure minime previste dalla normativa ai fini della tutela dei dati consente al titolare del trattamento di mettersi al riparo da sanzioni, la disciplina in commento è imperniata sull'innovativo principio della "responsabilizzazione" ("*accountability*"). In applicazione di tale principio, si impone ai titolari e responsabili l'adozione di comportamenti proattivi e tali da dimostrare di aver posto in essere, di volta in volta, tutte le misure tecniche ed organizzative che possano risultare adeguate ai fini della tutela dei dati, tenendo anche conto delle innovazioni tecnologiche che via via intervengano. Secondo la nuova normativa, occorre configurare il trattamento dei dati prevedendo fin dall'inizio (e, quindi, ancora prima di procedere al trattamento vero e proprio) le garanzie indispensabili per soddisfare i requisiti del GDPR e tutelare i diritti degli interessati con misure idonee ad impedire

possibili violazioni, con particolare riferimento ai sistemi elettronici (principi della "*privacy by design e by default*"). Ogni titolare, quindi, avrà in ogni momento la responsabilità dei propri sistemi e della loro adeguatezza ad evitare violazioni ed incidenti.

- **Valutazione d'impatto sulla protezione dei dati**: si tratta di un'analisi preventiva dei possibili rischi inerenti il trattamento dei dati con specifico riferimento all'attività concretamente esercitata, con cui si definiscono le carenze rispetto alla corretta gestione dei rischi medesimi e si indicano le misure per eliminare tali carenze e per prevenire e ridurre i rischi (con successivo controllo periodico degli effetti degli interventi a tal fine realizzati). Pur essendovi obbligati solo alcuni titolari di trattamento e quelli compresi nell'elenco che sarà redatto dal Garante, appare comunque opportuno per le imprese provvedere a redigere il "modello di prevenzione del rischio" (*Data Protection Impact Assessments*, in breve "**DPIA**"), finalizzato a rendere la tutela della privacy effettiva e parte dei sistemi sin dalla progettazione, nonché ad individuare le misure tecnico-organizzative idonee a ridurre i rischi. Si tratta, evidentemente, di una complessa attività di analisi e ridefinizione dei processi aziendali che comporta l'intervento di soggetti muniti di specifiche competenze di natura sia legale che tecnica.
- **Soggetti coinvolti**: il GDPR mantiene la figura del titolare del trattamento dei dati personali, ossia la persona fisica o giuridica, il servizio o altro organismo che, singolarmente o con altri, stabilisce le finalità e le modalità di utilizzo dei dati personali ed i relativi strumenti o misure di sicurezza da adottare. Il GDPR prevede la possibile contitolarità del trattamento ed il correlativo obbligo di definire il rispettivo ambito di responsabilità e compiti; fissa, inoltre, in modo dettagliato le modalità di designazione, da parte del titolare, di un responsabile del trattamento (soggetto persona fisica o giuridica, servizio o altro organismo che tratta dati personali per conto, appunto, del titolare del trattamento) e prevede obblighi specifici a carico del responsabile medesimo. Non prevede più espressamente la figura dell'incaricato del trattamento, ma non la esclude, facendo riferimento a "persone autorizzate al trattamento".
- **Il Responsabile per la Protezione dei Dati (*Data Protection Officer*, in breve "DPO")**: è una figura del tutto nuova introdotta dal GDPR. Ha ampi compiti di informazione, formazione, consulenza, valutazione d'impatto sulla protezione dei dati, sorveglianza e cooperazione con l'autorità di controllo. Anche se la designazione del DPO è obbligatoria solo in ipotesi specifiche (quando i trattamenti effettuati richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o quando le attività principali consistono nel trattamento su larga scala di particolari dati personali sensibili o relativi a condanne penali e reati), la sua nomina è opportuna in ogni caso, fungendo da consigliere del titolare e da controllore.
- **Registro dei trattamenti**: ogni titolare /responsabile del trattamento, con esclusione di imprese ed organizzazioni con meno di 250 dipendenti che non effettuano trattamenti a rischio, deve tenere un registro delle attività di trattamento (in cui si deve indicare, tra l'altro, il tempo di "retention", in quanto la disciplina in commento garantisce agli interessati il diritto all'oblio). Il Garante suggerisce l'adozione del registro in ogni caso, trattandosi di uno strumento fondamentale che

costituisce parte integrante di un sistema di corretta gestione dei dati personali, consentendo di disporre di un quadro aggiornato dei trattamenti in essere nell'azienda.

SANZIONI

Per la violazione della normativa in commento sono previste sanzioni amministrative molto onerose che possono arrivare:

- **fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale di gruppo** dell'esercizio precedente, per la violazione di obblighi del titolare e del responsabile e di altri organismi previsti dal GDPR;
- **fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale di gruppo** dell'esercizio precedente, per le violazioni dei diritti degli interessati.

Inoltre, è attribuita agli Stati la facoltà di prevedere sanzioni penali.

PROFILO OPERATIVO

Qualora lo richiediate, lo Studio Vi potrà affiancare nel processo di adeguamento alla nuova normativa unitamente ad un Legale esperto e qualificato in materia.

Cordiali saluti.