

ALESSIO BERTAGNIN & ASSOCIATI s.a.s.
Società tra Professionisti

Padova, 14 maggio 2018

Circolare n° 07/2018

Alla Spett.le Clientela

Oggetto: nuovo Regolamento Europeo in materia Privacy – **entrata in vigore 25/05/2018.**

Gentili Clienti, il **25 Maggio 2018** entrerà in vigore in tutti gli Stati membri della Comunità Europea il Regolamento UE/2016/679 noto come **GDPR** (General Data Protection Regulation) relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali.

CAMPO DI APPLICAZIONE

Tutte le Aziende aventi **almeno una sede operativa nell'UE**, che trattano in modo integrale o parziale i dati personali, indipendentemente dal fatto che il trattamento sia effettuato all'interno dell'Unione, dovranno adeguarsi alle nuove disposizioni facendo un'analisi della propria situazione rispetto ai dati gestiti, individuando le aree di intervento ed attivando le misure tecniche ed organizzative necessarie all'adeguamento degli standard previsti.

PRINCIPALI NOVITA' INTRODOTTE

Premesso che **Titolare del trattamento** è la persona fisica, l'impresa, l'ente, l'associazione, ovvero il soggetto, cui fanno capo effettivamente gli obblighi riguardanti il **trattamento di dati personali**. Egli determina le **finalità** ed i **metodi** di trattamento dei dati personali raccolti e adotta misure tecniche ed organizzative per garantire e dimostrare che il trattamento sia effettuato in conformità al Regolamento. E' sempre il Titolare a definire le politiche da adottare in materia di **protezione** dei dati personali.

Tra le numerose attività che le Aziende dovranno porre in essere, riteniamo utile segnalarVi in particolare:

- **Registro delle Attività di Trattamento:** tutti i Titolari ed i Responsabili del trattamento dovranno tenere un registro in forma scritta o elettronica delle operazioni di trattamento, sotto la propria responsabilità, che andrà esibito su richiesta del Garante. Le imprese con meno di 250 dipendenti sono esonerate dalla tenuta del registro dei trattamenti, a meno che il trattamento possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati sensibili o i dati relativi a condanne penali.
- **Valutazione d'impatto sulla protezione dei dati personali** ("Data Protection Impact Analysis" o "DPIA"): quando un determinato trattamento, tenuto conto dell'uso di nuove tecnologie e della sua natura, così come del contesto e delle finalità, possa presentare un rischio elevato per i diritti e libertà delle persone fisiche, il Titolare dovrà effettuare una **valutazione preliminare** d'impatto di quel trattamento sulla protezione dei dati. Questa valutazione è **sempre richiesta** quando si è in presenza di:
 - trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
 - trattamenti automatizzati, ivi compresa la profilazione;
 - trattamenti su larga scala di categorie particolari di dati (sensibili), nonché relativamente ai dati ottenuti dalla sorveglianza sistematica, sempre su larga scala, di zone accessibili al pubblico.
- **Nomina Responsabile della Protezione dei Dati – Data Protection Officer ("DPO"):** tale figura dovrà essere **obbligatoriamente** presente in tutte le aziende dove i trattamenti presentino specifici

ALESSIO BERTAGNIN & ASSOCIATI s.a.s.

Società tra Professionisti

rischi, ad esempio aziende dove ci sia tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale, o quelle che trattano “dati sensibili, genetici e biometrici”. Il DPO potrà essere un **dipendente interno o un soggetto esterno** avente con la società un contratto di servizi. Ogni azienda dovrà rendere noti i dati del proprio DPO e comunicarli al locale “Garante per la protezione dei dati personali”.

- **Obbligo di comunicazione in caso di violazione dei dati personali:** obbligo di comunicare l'avvenuta violazione di dati personali (c.d. Data Breach) per tutte le società che effettuino un trattamento di dati personali, notificando la violazione senza ingiustificato ritardo al Garante, **entro 72 ore** dal momento in cui ne è venuto a conoscenza. Qualora la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, invece, è previsto anche l'obbligo di comunicazione nei confronti di tutti gli interessati coinvolti.
- **Diritto all'oblio:** il Titolare ha l'obbligo di dar corso alla richiesta dell'interessato di **cancellazione dei suoi dati** personali e che questi non siano più sottoposti a trattamento quando non siano più necessari per le finalità per le quali sono stati raccolti, così come quando abbia ritirato il consenso o si sia opposto al trattamento o il trattamento dei dati personali non sia altrimenti conforme al Regolamento Europeo.
- **Diritto alla portabilità dei dati:** il Titolare ha l'obbligo di dar corso alla richiesta dell'interessato di **trasferire i dati** personali da un Titolare del trattamento ad un altro da lui indicato, senza alcun impedimento da parte del Titolare al quale sono stati forniti in precedenza i dati. I Titolari del trattamento, dovranno informare gli interessati dell'esistenza di tale nuovo diritto ed adempiere ai propri doveri senza ingiustificato ritardo (in ogni caso, entro un mese dal momento in cui è pervenuta loro la richiesta).

ASPETTO SANZIONATORIO

Per il mancato adeguamento potranno essere comminate **sanzioni amministrative pecuniarie** particolarmente elevate:

- fino a **10 milioni di Euro**, o per le imprese, fino al **2% del fatturato** globale annuo dell'esercizio precedente: per inosservanza degli obblighi del Titolare e del Responsabile del trattamento/inosservanza degli obblighi dell'organismo di certificazione/inosservanza degli obblighi dell'organismo di controllo.
- fino a **20 milioni di Euro**, o per le imprese, fino al **4% del fatturato** globale annuo dell'esercizio precedente: per inosservanza dei principi base del trattamento, dei diritti degli interessati, delle disposizioni sul trasferimento dei dati personali in paesi terzi o verso organizzazioni internazionali; di un ordine, limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'Autorità di controllo oppure di un ordine correttivo dell'Autorità di controllo.

Le sanzioni verranno applicate in funzione del singolo caso e tenendo conto della natura, della gravità e della durata della violazione, delle finalità del trattamento, del numero di interessati lesi, e del livello del danno, oltre ad altri elementi come il carattere doloso o colposo della violazione, ed anche delle misure adottate.

Il nostro Studio ha già intrapreso un percorso di pianificazione ed attuazione degli interventi essenziali per rispettare il nuovo regolamento affidandosi anche a competenti figure professionali esterne.

ALESSIO BERTAGNIN & ASSOCIATI s.a.s.
Società tra Professionisti

Le modifiche introdotte in materia di Privacy per le quali si è fornita una breve sintesi presentano elementi di una certa rilevanza e complessità che possono rendere necessario l'intervento di un esperto specializzato in materia. **Vi consigliamo perciò, qualora non abbiate già provveduto all'adeguamento, di contattare soggetti specializzati che Vi assistano nelle operazioni di aggiornamento necessarie.**

Restiamo a disposizione per fornirVi il supporto che riterrete necessario e porgiamo

Cordiali Saluti
Il Cdl Alessio Bertagnin