Brescia, lì 21.05.2018

SPETT.LE CLIENTE

Oggetto:

NUOVO REGOLAMENTO PRIVACY IN VIGORE DAL 25.05.2018

Il 25 maggio 2018 diverrà definitivamente applicabile il Regolamento UE n. 2016/679 (c.d. GDPR). Tale normativa andrà a modificare l'attuale assetto legislativo in materia privacy di cui al D.lgs 196/2003 (c.d. Codice Privacy). Si rende pertanto necessario procedere ad un adeguamento della gestione del trattamento dei dati personali, in modo tale da ottenere una *compliance* aziendale conforme alle nuove disposizioni previste dal legislatore europeo.

Per maggiore chiarezza, di seguito sono elencate le principali novità introdotte dal GDPR.

- **SOGGETTI**

Il GDPR modifica l'Organigramma Privacy. Permane la figura del Titolare del trattamento, che corrisponde alla persona, fisica o giuridica, che determina le finalità e i mezzi del trattamento. Il Responsabile del trattamento, che agisce per conto del Titolare, è esterno all'azienda. Ciò è dovuto al fatto che i Responsabili sono chiamati a rispondere in solido con il Titolare per l'intero ammontare del danno qualora la responsabilità dello stesso sia da attribuire ad entrambi. In luogo dei Responsabili interni sussistono i Delegati al trattamento da parte del Titolare, preposti a garantire la sicurezza nella gestione dei dati nelle singole aree aziendali (es: settore HR, marketing…)

- **MISURE DI SICUREZZA ADEGUATE AL RISCHIO**

Il GDPR richiede che vengano predisposte misure di protezione del dato "adeguate" rispetto al rischio. Di volta in volta, sulla base della singola realtà aziendale, si renderà necessario analizzare la tipologia del dato trattato, le possibilità di violazione/cancellazione/modificazione dello stesso e le conseguenti misure di sicurezza. Non è pertanto più sufficiente attenersi alle misure minime di sicurezza previste dall'Allegato B al D.lgs 196/2003

- **PRIVACY BY DESIGN**

Le imprese, come requisito strutturale del sistema, devono garantire la protezione dei dati personali facendo ricorso alle misure tecniche e organizzative adeguate, prevenendo l'eventuale violazione o distruzione dei dati

- **PRIVACY BY DEFAULT**

Le imprese devono trattare, per impostazione predefinita, solamente i dati strettamente necessari per il raggiungimento di specifiche finalità. Occorre, pertanto, che il sistema di trattamento garantisca la non eccessività dei dati raccolti

- **VALUTAZIONE PREVENTIVA DEL RISCHIO (DPIA)**

L'impresa è tenuta a svolgere una valutazione preliminare dell'impatto di un trattamento sulla privacy e la sicurezza dei dati ogni volta che un trattamento, effettuato ricorrendo alle nuove tecnologie, ponga in serio pericolo i dati personali. La valutazione di impatto rientra tra gli strumenti di prevenzione richiesti dal legislatore europeo che, accanto ai nuovi concetti di *privacy by design* e *by default*, intende far sì che le aziende si adoperino, fin dal momento della ricezione, per impedire la violazione dei dati personali delle persone fisiche

- **DATA BREACH**

Qualora, nonostante siano state prese tutte le misure del caso, si verifichi una violazione dei dati, l'impresa è tenuta a comunicarlo all'Autorità di Controllo (Garante Privacy) senza ritardo ingiustificato e comunque entro 72 ore dalla scoperta. La comunicazione non è dovuta nel caso in cui risulti improbabile che la violazione costituisca un rischio per le libertà e i diritti della persona fisica.

Per quanto riguarda l'interessato, questi non ha diritto a ricevere sempre e comunque la comunicazione della violazione dei suoi dati, che è dovuta solamente nel momento in cui la violazione ponga in essere un serio rischio ai diritti e alle libertà degli interessati

- **REGISTRO DEI TRATTAMENTI**

Ogni Titolare e Responsabile del trattamento deve tenere il Registro dei trattamenti. Questo documento contiene l'indicazione rispettivamente delle attività di trattamento svolte sotto la propria responsabilità e quelle compiute su disposizioni del Titolare. Il Registro costituisce applicazione del principio di accountability, in ordine al quale ciascun Titolare del trattamento si assume pienamente la responsabilità della gestione dei dati personali; su di lui incombe l'onere di provare di aver adottato tutte le misure idonee a garantire una gestione del dato conforme alla disciplina europea. La tenuta del Registro non è obbligatoria per tutti i Titolari e Responsabili, ma solo per le imprese e le organizzazioni dotate di almeno 250 dipendenti, salvo che il trattamento che effettuano ponga in pericolo i diritti e le libertà degli interessati ovvero non sia occasionale o includa dati particolari o giudiziari

- **PERIODO DI CONSERVAZIONE DEI DATI**

A differenza del Codice Privacy, l'art. 13 del GDPR impone di indicare nell'informativa privacy l'indicazione del periodo massimo di conservazione dei dati personali, ovvero i criteri utilizzati per la determinazione di tale periodo. I dati non potranno più essere conservati senza limiti di tempo, ma solamente per un periodo di tempo adeguato rispetto alle finalità perseguite, secondo le disposizioni di legge e le indicazioni del Garante Privacy

- **ESERCIZIO DEI DIRITTI DELL'INTERESSATO**

Il GDPR allarga il novero dei diritti riconosciuti all'interessato: l'art. 20 introduce il diritto alla portabilità dei dati, ossia il diritto ad ottenere i dati che lo riguardano in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasferirli ad un nuovo Titolare del trattamento senza alcun impedimento. Più ampio rispetto alla normativa del Codice Privacy è il diritto alla cancellazione od oblio (art. 17), che impone al Titolare cui è stata imposta la cancellazione dei dati e che precedentemente li aveva resi pubblici di informare i Titolari che li gestiscono al fine di ottenere la cancellazione di ogni link, copia o

riproduzione dei dati. L'art. 18 tratta della limitazione al trattamento, per cui il trattamento può non soltanto essere impedito, ma solamente limitato a richiesta dell'interessato e alla presenza degli specifici requisiti di legge.

Davanti alle richieste dell'interessato, il Titolare del trattamento è tenuto a rispondere all'interessato senza ingiustificato ritardo e comunque entro 1 mese (prorogabile di due mesi nei casi di particolare complessità), anche nel caso di diniego.

- **SANZIONI**

Assumono particolare rilevanza le nuove sanzioni previste dal GDPR, ben più gravose rispetto al sistema sanzionatorio del Codice Privacy. Il Titolare può essere tenuto a versare, quale sanzione amministrativa pecuniaria, da un minimo di 10.000,00 euro e un massimo pari al 4% del fatturato globale totale annuo dell'esercizio precedente

- **ONE STOP SHOP (c.d. SPORTELLO UNICO)**

Le imprese che operano in più Stati membri potranno rivolgersi al Garante Privacy del Paese dove hanno la sede principale. Una Società che opera in più Paesi può scegliere di trattare con l'Autorità di Controllo di un Paese scegliendo un'Autorità di Controllo Capofila (c.d. Lead Authority), anziché dove gestire un'Autorità di Controllo in ciascun Paese in cui opera.

Restiamo a disposizione per ogni precisazione o chiarimento in ordine ai punti sopra esposti.

Studio Dott. Begni & Associati