GILI - STAGNO & PARTNERS

"COMMERCIALISTI ASSOCIATI"

DAVIDE GILI
ANDREA SIGNORINI
GENNARO STAGNO

PIAZZALE L. CADORNA, 13 - 20123 MILANO
TEL. +39 02 86.99.56.57 FAX +39 02 89.09.55.80
E-MAIL INFO@GILISTAGNOPARTNERS.IT
WWW.GSPARTNERS.IT

Nostra Circolare Informativa N. 3 / 2018

A tutti i clienti
Loro sedi

Milano, lì 23 Maggio 2018

***Oggetto*: Nuove norme in materia di Privacy: GDPR.**

INTRODUZIONE

A partire dal 25 maggio 2018 entrano in vigore le nuove norme previste dal Regolamento europeo 2016/679 relativo alla "protezione delle persone fisiche con riguardo al trattamento dei dati personali* e la libera circolazione di tali dati".

Con tale Regolamento, noto come GDPR ("General Data Protection Regulation"), si introducono novità molto significative alle modalità di gestione dei dati personali di tutti i cittadini della Unione Europea.

Vengono introdotti nuovi diritti per i cittadini e nuovi obblighi per i soggetti che gestiscono questi tipi di dati (aziende e professionisti), sanzionati molto pesantemente.

Senza voler entrare in tutti i dettagli contemplati dalla nuova, complessa legislazione, vediamo quali sono le più importanti novità previste.

CONSENSO

Per i dati sensibili** e per alcune altre tipologie di dati, il consenso deve essere esplicito, il che non vuol dire che debba necessariamente essere dato per iscritto, anche se questa è la forma più idonea a dimostrarlo. Il consenso dei minori è valido a partire dai 16 anni.

** Dati Personali: qualsiasi informazione che identifica o rende identificabile una persona fisica o che possa descrivere uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*

*** Dati Sensibili: dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati relativi alla salute, alla vita sessuale o all'orientamento sessuale.*

CONTENUTI, TEMPI E MODALITA' DELL'INFORMATIVA

I contenuti dell'informativa sono più ampi rispetto alle norme precedenti: vanno specificati i dati di contatto del Responsabile, la base giuridica del trattamento, l'interesse legittimo, il periodo di conservazione dei dati o i criteri stabiliti per stabilire tale periodo, e il diritto di presentare reclamo all'autorità di controllo.

Qualora i dati personali non siano raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro un termine ragionevole (e comunque non oltre un mese) dalla raccolta.

L'informativa dovrà essere concisa, trasparente, intelligibile per l'interessato e facilmente accessibile, utilizzando un linguaggio chiaro e semplice. Deve essere data in linea di principio per iscritto e preferibilmente in formato elettronico, ma sono ammessi altri mezzi.

DIRITTI DEGLI INTERESSATI

Il diritto di accesso prevede in ogni caso il diritto di ricevere una copia dei dati personali oggetto del trattamento.

Il diritto di cancellazione (diritto all'oblio) consiste nel diritto alla cancellazione dei propri dati personali con l'obbligo (in caso di dati "resi pubblici") di informare della richiesta di cancellazione altri eventuali titolari che trattano i dati cancellati.

Viene ampliato anche il già esistente diritto di limitazione e blocco del trattamento e viene introdotto il diritto alla portabilità dei dati per i trattamenti "automatizzati" ma solo con il consenso dell'interessato.

TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO

Con riferimento alle figure già esistenti del Titolare e del Responsabile del trattamento dei dati personali, viene introdotta la possibilità della contitolarità del trattamento, con l'obbligo di definire i rispettivi ambiti di responsabilità; vengono inoltre fissate più dettagliatamente le caratteristiche dell'atto con cui il titolare designa un responsabile.

Viene inoltre resa obbligatoria la figura del Responsabile della Protezione dei Dati (Data Protection Officer, DPO), nelle aziende pubbliche ed in tutte le aziende dove i trattamenti presentino specifici rischi. Varie regole sono previste per tale figura che diventa obbligatoria per molte tipologie di aziende.

REGISTRO DEI TRATTAMENTI

Viene introdotto l'obbligo della tenuta del Registro dei Trattamenti, ma solo per i soggetti con più di 250

dipendenti, a meno che non effettuino trattamenti a rischio. Il registro è pensato come strumento fondamentale per ogni valutazione ed analisi del rischio anche ai fini di un'eventuale supervisione da parte del Garante.

MISURE DI SICUREZZA E NOTIFICA DI VIOLAZIONI DI DATI PERSONALI

Il regolamento introduce con forza il concetto di "responsabilizzazione" di titolari e responsabili, che dovranno adottare comportamenti proattivi tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento stesso, ad esempio attraverso la Valutazione d'impatto sulla protezione dei dati personali "DPIA" prevedendo fin dall'inizio le garanzie indispensabili per tutelare i diritti degli interessati nonché prevedendo una serie di attività per valutare i rischi inerenti al trattamento ed attuare le misure necessarie per mitigare tali rischi.

Le misure di sicurezza attuate devono garantire un livello adeguato al rischio del trattamento. Non sono previsti obblighi di adozione di misure "minime" di sicurezza ma tale valutazione viene lasciata caso per caso al titolare ed al responsabile.

D'ora in poi tutti i titolari (indipendentemente dal tipo di settore) dovranno notificare all'Autorità di controllo le eventuali violazioni di dati di cui vengono a conoscenza, entro 72 ore, ma soltanto se ritengono che da tale violazione ne possano derivare dei rischi per i diritti e le libertà degli interessati. Se la probabilità di tale rischio è elevata, si dovranno informare anche gli interessati.

SANZIONI

Le sanzioni previste dal nuovo regolamento variano in funzione di vari criteri, come la natura, la gravità e la durata della violazione come pure il danno arrecato, la dimensione dell'azienda, il carattere doloso o colposo, e tanti altri elementi.

Quello che è certo è che possono arrivare anche a 10.000.000 di euro od al 2% del fatturato dell'azienda.

Anche per questo motivo non si tratta sicuramente di adempimenti da sottovalutare.

Lo studio rimane a disposizione per ogni eventuale chiarimento in merito.

GILI – STAGNO & PARTNERS