I nuovi adempimenti in materia di protezione dei dati personali GDPR, General Data Protection Regulation - Regolamento (UE) 2016/679

Di Luana Messina – Ingegnere Edile

Il Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in abrogazione della direttiva 95/46/CE, entrerà in vigore il 25 maggio 2018, imponendo obblighi stringenti alle imprese in materia di trattamento e di gestione dei dati personali. Le nuove disposizioni rafforzeranno significativamente il regime di tutela dei dati personali e troveranno applicazione sia presso le aziende con sede legale o operativa nell'Unione Europea sia presso quelle che, pur essendo stabilite al di fuori dall'Europa, trattino dati relativi a cittadini di uno Stato membro. Con il nuovo Regolamento si passerà ad un sistema di *governance* dei dati personali basato su un'alta responsabilizzazione del soggetto che opera il trattamento*,* cui verrà richiesta la capacità di prevenire errori e di dimostrare, tramite idonea documentazione, l'adozione di appropriate policy interne. Nell'ambito di ciascuna organizzazione aziendale, il tema della protezione dei dati personali dovrà diventare presupposto imprescindibile da considerare già nella fase di progettazione di processi, di servizi e/o di prodotti che implichino il trattamento di tali dati. Non saranno più previste misure "minime" di sicurezza, mentre verrà introdotto l'obbligo di adottare misure tecniche organizzative adeguate al rischio, con l'istituzione di meccanismi di certificazione della protezione dei dati al fine di dimostrare la conformità al Regolamento dei trattamenti effettuati da Titolari e Responsabili.

Tra le novità previste dal Regolamento, risultano di particolare rilevanza le seguenti:

- ***Registro delle attività di trattamento***. I Titolari e i Responsabili saranno obbligati a istituire un apposito registro, in forma cartacea ed elettronica, in grado di offrire un quadro aggiornato dei trattamenti effettuati all'interno delle azienda, strumento indispensabile per ogni valutazione e analisi dei rischi connessi agli stessi. L'obbligo di istituzione del registro delle attività di trattamento non opererà per le società e per gli enti con meno di 250 dipendenti, ma solo nel caso in cui questi non operino trattamenti di dati personali a rischio per diritti e le libertà dell'interessato o che includano categorie particolari di dati personali e relativi alle condanne penali e ai reati.

- ***Analisi dei rischi.*** Il Titolare e il Responsabile dovranno effettuare un'analisi dei rischi derivante dal tipo di trattamento che intendono porre in essere. Verranno quindi valutati, tipicamente, i rischi di distruzione, perdita, modifica, divulgazione non autorizzata o accesso indesiderato ai dati oggetto di trattamento.

- ***Valutazione d'impatto.*** Qualora un trattamento possa potenzialmente compromettere i diritti e le libertà delle persone fisiche interessate, il Titolare sarà chiamato ad effettuare una valutazione d'impatto specifica, analizzando i rischi prevedibili e le misure tecniche e organizzative che il Titolare intenderà adottare per la loro mitigazione. La valutazione d'impatto dovrà contenere una descrizione sistematica dei trattamenti previsti e delle loro finalità, oltre a una valutazione documentata in merito alla necessità e alla proporzionalità dei trattamenti in relazione alle finalità perseguite. Qualora all'esito della valutazione il Titolare ritenga che il trattamento presenti un rischio elevato, lo stesso sarà tenuto a consultare l'Autorità di Controllo, adottando le misure eventualmente imposte per la mitigazione del rischio.

- ***Responsabile della protezione dei dati - DPO (Data Protection Officer).*** Tale figura sarà volta a facilitare il rispetto delle disposizioni dettate dal Regolamento, pur non assumendo profili di responsabilità specifica. La sua funzione sarà meramente consultiva in materia di strategie e criteri di protezione dei dati personali assunti in azienda. La designazione del DPO sarà obbligatoria in caso: di trattamento effettuato da un'Autorità pubblica o da un organismo pubblico; monitoraggio regolare e sistematico degli interessati su larga scala; trattamento su larga scala di dati sensibili e giudiziari.

In merito ai profili sanzionatori, il Responsabile del trattamento sarà direttamente passibile di sanzioni amministrative, rispondendo direttamente per il danno causato, tanto nell'ipotesi di mancata osservanza delle disposizioni del Titolare, quanto in quella di inadempimento agli obblighi previsti dal Regolamento. I trattamenti effettuati dal Responsabile dovranno essere disciplinati all'interno di un contratto che vincoli lo stesso al Titolare, indicando la materia disciplinata, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di dati degli interessati, gli obblighi e i diritti del Titolare. Nell'ipotesi in cui il Titolare e il Responsabile siano coinvolti nello stesso trattamento svolto in violazione alle disposizioni di legge, entrambi saranno chiamati a rispondere in solido per l'intero ammontare del danno causato. Sanzioni fino a € 20.000.000,00 o, nel caso di imprese, al 4 % del fatturato globale annuo si applicheranno nel caso di:

- violazione dei principi del trattamento, incluse le condizioni per il consenso;

- violazione dei diritti degli interessati;

- inosservanza delle norme in tema di trasferimento internazionale dei dati;

- violazione degli obblighi previsti dalle legislazioni degli Stati membri;

- inosservanza di un ordine di limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi dei dati imposto dall'autorità di controllo, o diniego di accesso all'autorità medesima.

Sanzioni di importo massimo pari a € 10.000.000,00 o al 2% del fatturato globale annuo si applicheranno in caso di violazione degli obblighi previsti in capo al Titolare e al Responsabile, all'organismo di certificazione e all'organismo di controllo. Quanto alle sanzioni penali, queste saranno direttamente demandate alle singole legislazioni degli Stati membri.