La protezione dei dati:

Il nuovo Regolamento EU 2016/679

Il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il Regolamento EU 2016/679, entrato in vigore il 24 maggio 2016, ma applicabile a decorrere dal ***25 maggio 2018***. La riforma Europea è composta da tre provvedimenti fondamentali:

- Il Regolamento UE 2016/679
- La Direttiva UE 2016/680
- La Direttiva UE 2016/681

Il nuovo quadro normativo elaborato congiuntamente dal Parlamento e dal Consiglio Europeo, rappresenta in generale, un passo importante verso una più ampia e funzionale protezione delle persone fisiche e della sfera personale riguardante dati sensibili e personali. L'articolo 13 del Regolamento dispone che, al fine di ***"assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possano ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca la certezza del diritto"***.

Il Nuovo Regolamento EU 2016/679 si compone di un **nuovo sistema di gestione della *privacy*** il quale si articola in quattro punti focali:

- Il principio dell'***Accountability***

In generale, il termine di origine anglosassone "*Accountability*" letteralmente traducibile con "rendicontazione", fa riferimento a un approccio pratico e concreto in tema di protezione dei dati personali, il quale, per il titolare del trattamento si concretizza in due obiettivi fondamentali:

- Poter garantire all'interno della propria organizzazione, procedure e misure adeguate che vadano a comporre un modello di gestione della *privacy* funzionale;

- Poter garantire all'esterno, verso i terzi, un modello di gestione della propria "*Accountability*", il quale risulti conforme alle disposizioni di legge e all'occorrenza utilizzabile come prova, anche dinanzi all'Autorità di Controllo. Di conseguenza, ne deriva che, il principio di *accountability* sia strettamente connesso a quello di trasparenza. (Art. 5, comma 2). Il soggetto preposto dalla disciplina comunitaria a sovraintendere un determinato

modello di gestione *privacy* è il ***Data Protection Officer*** **(D.P.O.).** Tale figura ha il compito di fornire l'assistenza necessaria per progettare, verificare e mantenere un sistema di gestione dei dati personali.

- La ***Data Protection Impact Assessment*** (D.P.I.A)

L'istituto della valutazione d'impatto sulla protezione dei dati personali, riguarda ogni tipo di trattamento il quale presenti un potenziale rischio per i diritti e le libertà delle persone fisiche. La valutazione viene effettuata sulla base di alcuni parametri, come la natura dei dati, la tipologia e la finalità del trattamento. Il titolare del trattamento prima di procedere deve effettuare, quindi, una valutazione dell'impatto che i trattamenti previsti avranno sulla protezione dei dati personali; la D.P.I.A. è obbligatoria quando sono trattati dati sensibili o giudiziari, nei casi di trattamenti automatizzati e nei casi di profilassi (Art 35). Tale procedura è un'attività propedeutica alla progettazione di sistemi conformi ai principi di privacy by design e by default.

- La ***'privacy by design' e by 'default'***

In generale, essi consistono nell'introduzione del principio secondo cui qualsiasi progetto che includa aspetti della privacy, debba essere realizzato fin dalla prima fase della progettazione, secondo modelli di gestione conformi alla normativa Europea.

Nello specifico, definire la privacy by default va ad indicare che, il titolare dei dati personali i quali vengono raccolti in occasione di registrazioni a servizi telematici o della stipulazione di contratti, o in ogni caso in cui un individuo renda i propri dati ad un terzo, questi siano trattati sempre attraverso un percorso di politica aziendale o amministrativa interna che ne tuteli la diffusione.

Mentre, con la terminologia privacy by design, s'intende, la necessità di tutelare il dato sin dalla progettazione di sistemi informatici che ne prevedano l'utilizzo. Così facendo, I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità (Art 25).

- La ***Data Breach Notification***

Una progettazione funzionale di un sistema per la privacy è il presupposto fondamentale per evitare o attenuare danni derivanti da una *data breach*. In capo ai titolari del trattamento, infatti, sorge un obbligo generalizzato di comunicazione delle violazioni dei dati personali. Quest'ultima dovrà avvenire senza ingiustificato ritardo e entro le 72 ore dal momento in cui il titolare ne è venuto a conoscenza, notificando la violazione al Garante (Art 33).

Illeciti e sanzioni

Il sistema sanzionatorio previsto dal Codice della Privacy è il sistema c.d. a "doppio binario", il quale distingue tra violazioni amministrative ed illeciti penali. La previsione di una sanzione, anche di tipo penale, è giustificata dall'esigenza di tutelare un bene di rango Costituzionale, quale quello della riservatezza e per la quale le sanzioni amministrative pecuniarie non hanno un reale effetto dissuasivo, specie nei confronti delle organizzazioni di media-grande entità.

Con l'introduzione del Regolamento UE 2016/679, all'interno del sistema sanzionatorio, si è avuto un aumento dell'ammontare delle sanzioni amministrative-pecuniarie. Ne segue che, un trattamento non conforme alla legge potrà comportare, a seconda dei casi:

- ***Sanzioni penali***: tale tipologia di sanzioni rimane di competenza dei singoli Stati Membri.

- ***Sanzioni amministrative***: le sanzioni di tipo amministrative-pecuniarie ammontano fino a 20 milioni di euro, o in caso di un'impresa, **fino al 4% del fatturato totale annuo** mondiale dell'esercizio precedente, se superiore. Nella decisione di infliggere una sanzione e quantificare il suo importo, alcuni criteri fondamentali fungeranno da parametro.

- ***Responsabilità civile***: ai sensi dell'articolo 82 del Regolamento 2016/679: ***"chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento"***. L'articolo 82 UE afferma, dunque, il diritto di ottenere il risarcimento del danno, sia patrimoniale sia quello non patrimoniale. Tale diritto sorge nel momento in cui venga posta in essere una condotta che costituisca una violazione del regolamento. Il soggetto che sarà tenuto al risarcimento è il titolare del trattamento o il responsabile del trattamento.