Cosa impone il GDPR 679/2016? Risponde l'avvocato Maria Cupolo

a cura della Redazione

L'entrata in vigore del Regolamento Europeo sulla tutela dei dati personali, il GDPR 679/2016, delinea degli adempimenti da parte dei titolari del trattamento anche di natura tecnologica, per disporre di "sistemi adeguati" per la sicurezza dei dati. Quali sono i riferimenti della norma al riguardo?

L'entrata in vigore del Regolamento Europeo sulla tutela dei dati personali, il GDPR 679/2016 che sarà applicabile in tutti gli stati membri a partire da maggio 2018, delinea in effetti un approccio nuovo rispetto all'attuale disciplina, un approccio che richiama tutta una serie di adempimenti anche di natura tecnologica.

Ci si spiega meglio: la nuova disciplina per la protezione dei dati personali, pone al centro la figura del Titolare al quale si richiede prima di tutto un onere e un ruolo di responsabilizzazione ovvero di ***"accountability"***.

Il titolare del trattamento dei dati deve essere in grado di dimostrare di avere adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi: deve dimostrare cioè in modo positivo e proattivo che i trattamenti dei dati effettuati sono adeguati e conformi al Regolamento.

Insomma "dalla forma alla sostanza", verrebbe da dire.

Occorrerà ripensare infatti, con una nuova visione e in maniera decisamente più "attiva", alle modalità di gestione e dunque trattamento e utilizzo dei dati personali attraverso una sempre maggiore responsabilizzazione nonché adottando quell'insieme di strumenti anch'essi delineati dalla nuova disciplina, strumenti quali, primo fra tutti, l'adozione delle misure di sicurezza ovvero di quelle misure *"tecniche ed organizzative" al fine di prevenire ed arginare i rischi del trattamento quali "la distruzione accidentale o illegale, la perdita , la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque*

elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale".

Ma vi è di più: il Regolamento all'art. 25 comma 1 delinea inoltre il principio della **privacy by design** in base al quale: *"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati"*.

Il titolare del trattamento dovrà, dunque, fin dalla fase di progettazione, effettuare una valutazione del trattamento dei dati che intende avviare e dovrà adottare tutte e proprio "quelle misure e quegli accorgimenti" che consentono di operare in linea con la normativa di riferimento.

L'applicazione del principio della *privacy by design* richiederà inevitabilmente anche un coinvolgimento di coloro che

sviluppano e progettano prodotti, servizi e applicazioni da cui possa derivare un trattamento di dati personali; tali strumenti e servizi, infatti, devono essere progettati e sviluppati tenendo conto della normativa in materia di protezione dei dati e devono avere caratteristiche tali da consentire ai Titolari del trattamento di adempiere agli obblighi prescritti dalla normativa stessa.
Accountability e approccio by design debbono accompagnare dunque il Titolare ed anche il responsabile del trattamento che, così come indicato dall'art. 32 del regolamento *"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche"* devono adottare le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Queste misure non più delineate e tipizzate come per l'attuale Codice privacy, comprendono tra le altre come pure indicato nello stesso art. 32:

a) *la pseudonimizzazione e la cifratura dei dati personali;*

b) *la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*

c) *la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*

d) *una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*

La protezione dei dati e la sicurezza andranno pertanto gestite dal titolare ma anche dal responsabile del trattamento, attraverso la gestione del rischio che deriva proprio da una valutazione ed adozione delle misure tecnologiche nonché dall'adozione di una gestione adeguata a quelli che sono i processi con uno sguardo ai profili ed ai modelli organizzativi e contrattuali.

L'importanza della valutazione del rischio e dell'adozione nonché attenzione sulle misure di contenimento ovvero quelle misure "adeguate" inevitabilmente ci riportano anche ad una imprescindibile necessità di guardare con attenzione al tipo di investimenti che occorrerà fare in un'ottica di opportunità, ottimizzazione e consapevolezza per un sempre più elevato ed adeguato livello di "sicurezza".

Quali sono gli aspetti sanzionatori previsti dal GDPR in caso di accertato inadempimento da parte del titolare del trattamento?
Le sanzioni peseranno non poco, senza entrare nelle singole fattispecie è doveroso sottolineare e osservare come la formulazione del sistema sanzionatorio che emerge dal nuovo Regolamento, porti ad un innalzamento dei massimi che verranno applicati.
Il Regolamento individua infatti due fasce: la prima ha come massimo edittale l'importo di 10 milioni di euro e la seconda 20 milioni di euro. Senza contare che tali cifre possono ulteriormente incrementarsi per le imprese, se si applica la sanzione in misura percentuale, pari rispettivamente al 2% o al 4% del fatturato mondiale globale annuo. Nell'ambito del procedimento sanzionatorio avrà pertanto più che mai importanza la necessità di dare evidenza e dunque dimostrare di aver fatto quanto dal Regolamento richiesto anche e soprattutto in punto all'applicazione di quelle misure tecniche ed organizzative "adeguate" al rischio ed all'applicazione di un adeguato programma di compliance.

In che modo può essere ritenuto corresponsabile il fornitore di sistemi ed a quali rischi è esposto?
L'art. 32 del regolamento non sottolinea il ruolo del solo Titolare del trattamento ma anche del responsabile ivi inclusi pertanto i responsabili esterni.
C'è una vera e propria evoluzione da un punto di vista legale-tecnologico che richiede, anche alla luce della previsione di una responsabilità solidale dei soggetti coinvolti, un'attenzione particolare al rapporto con i fornitori andando ad individuare le responsabilità e "chi deve fare cosa" essendo, si ribadisce, anche i fornitori, quali responsabili, chiamati ad avere un ruolo attivo e consapevole nell'applicazione delle misure "adeguate".