a cura di ELENA TROTTA

NUOVO REGOLAMNETO SULLA PRIVACY

Il 4 maggio 2016 è stato pubblicato nella ***Gazzetta Ufficiale dell'Unione Europea*** *il nuovo* ***Regolamento (UE) 2016/679*** *del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione ditali dati e che abroga la direttiva 95/46/CE(regolamento generale sulla protezione dei dati)* ***da cui era disceso il D.Lgs. 196/2003.***

Si tratta di ***una piccola rivoluzione nel mondo della privacy****, attesa ormai da diversi anni e il cui percorso è stato in continua salita, essendoci in gioco milioni di euro legati soprattutto alle attività di marketing e di profilazione oltre che i rapporti tra Europa e resto del mondo (con Stati uniti, Canada e Cina principali interlocutori interessati).*

Ma cosa cambia realmente:

1 – Individuazione dei soggetti a cui si applica il Regolamento

Prima = *la normativa era applicabile nel luogo in cui aveva sede il Titolare del trattamento dei dati.*

Con il Nuovo Regolamento Europeo = *la legge applicabile è quella del soggetto i cui dati vengono raccolti. Social network, piattaforme web e motori di ricerca saranno quindi soggetti alla normativa europea anche se sono gestiti da società con sede fuori dall'UE. Con il nuovo regolamento viene abolita la figura del Titolare del Trattamento Dati e rimane solo la figura di Responsabile.*

2 – Dovere di documentazione e informazione

Prima = *la documentazione era importante.*

Con il Nuovo Regolamento Europeo = *principio dell'accountability (responsabilità verificabile), secondo cui tutti i soggetti che partecipano al trattamento dati devono essere consci e responsabili e devono tenere documentazione di tutti i trattamenti effettuati. Chi non documenta, è soggetto a possibili sanzioni: a prescindere dall'utilizzo che si fa dei dati, è sufficiente non avere i documenti per essere perseguibili.*

3 – L'informativa privacy

Prima = *l'informativa era spesso lunga, incomprensibile e con richiami normativi complessi.*

Con il Nuovo Regolamento Europeo = *l'informativa deve essere leggibile, comunicativa, accessibile, concisa e scritta con linguaggio chiaro e semplice con un numero limitato di riferimenti normativi. Deve essere fornita per iscritto (oralmente va bene SOLO se l'interessato è d'accordo e la sua identità deve comunque essere comprovata con altri mezzi). Si propone anche l'utilizzo di icone per rendere l'informativa leggibile anche da parte di chi non conosce la lingua.*

4 – Cambia il consenso

Prima = *il consenso doveva essere libero, specifico e informato. Ci doveva essere un atto formale per accettare il trattamento dei dati.*

Con il Nuovo Regolamento Europeo = *il consenso deve essere libero, specifico, informato e inequivocabile. Il consenso è valido se la volontà è espressa in modo NON equivoco, anche con un'azione positiva: non ci deve essere per forza la casella di spunta, basta un testo in cui si informa che proseguendo si accetta il trattamento dati con link all'informativa.*

5 – Valutazione d'impatto sulla protezione dei dati

Prima = *si preparava il DPS.*

Con il Nuovo Regolamento Europeo = *si effettua una valutazione degli impatti privacy analizzando i rischi, definendo i gap rispetto alla corretta gestione dei rischi, stabilendo un piano per colmarli e controllando annualmente gli effetti degli interventi per ridurre i rischi. Quasi sicuramente il nuovo documento sarà chiamato PIA: Privacy Impact Assessment.*

6 – Abolizione della notificazione

Prima = *si doveva informare il Garante che un soggetto sta trattando dati per una particolare finalità. (ex art. 37 D.lgs. 196/2003)*

Con il Nuovo Regolamento Europeo = *non si dovrà più notificare il Garante, ma ogni anno l'azienda dovrà redigere il privacy impact assessment, con il quale si considera effettuata la notifica.*

7 – Il Data Protection Officer

Prima = *il DPO non era una figura contemplata.*

Con il Nuovo Regolamento Europeo = *bisogna istituire (per tutti gli enti pubblici e per aziende il cui core business coinvolge trattamenti di natura rischiosa) un* ***responsabile per la protezione dei dati.*** *Il DPO sarà una figura manageriale con rinnovo periodico, sarà referente del Garante e dovrà avere requisiti e competenze elevate. Il DPO potrà essere sia un dipendente che un collaboratore con regolare contratto.*

8 – Privacy by design e Privacy by default

Prima = *la privacy era un elemento conclusivo e finale.*

Con il Nuovo Regolamento Europeo = *la privacy deve essere vista come un elemento iniziale: devo pensarci appena decido di raccogliere dati e predisporre alti livelli di privacy nel trattamento dati, che potranno essere abbassati dal diretto interessato.*

9 – Obbligo di segnalazione in caso di violazione dei dati

Prima = *non era necessario comunicare violazioni nel trattamento dati.*

Con il Nuovo Regolamento Europeo = *nel caso di violazione del trattamento dati bisogna effettuare una segnalazione al Garante entro 72 ore dall'evento e, nel più breve tempo possibile, bisogna informare anche i diretti interessati.* ***Il mancato rispetto di quest'obbligo comporta sanzioni penali****. È possibile prevedere delle assicurazioni per coprire il costo di comunicare la violazione a tutti gli interessati, definito Data Breach.*

10 – Riconoscimento di nuovi diritti

Prima = *pochi diritti che tutelavano l'interessato in merito alla gestione dei suoi dati.*

Con il Nuovo Regolamento Europeo = *nuovi diritti:* ***diritto alla portabilità dei dati*** *(posso pretendere che il soggetto a cui ho concesso l'uso dei miei dati me li restituisca su un supporto elettronico strutturato così che io possa farne ulteriore uso, anche presso un altro fornitore), diritto a essere totalmente dimenticato da chi ha raccolto i miei dati.*

Inoltre vi sono altre importati novità:

- *Vengono introdotte le definizioni di "Dato Generico" e "Dato Biometrico"*
- *Introdotta la categoria del trattamento dati dei minori*
- *Introduzione della Cotitolarità nel trattamento dei dati*
- *Introduzione del Diritto all'Oblio*
- *Introduzione della figura del Joint Controller*
- *Introduzione di requisiti più stringenti per trasferire dati verso Paesi TerziIntroduzione del principio dell'applicazione del diritto UE anche ai trattamenti di dati personali non svolti nell'UE, se relativi all'offerta di beni e servizi ai cittadini UE o tali da permettere il monitoraggio dei comportamenti dei cittadini dell'UE*
- *Istituzione del Comitato Europeo per la protezione dei Dati*

LO SCADENZIARIO DELL'ALBERGATORE

- ✓ ***Non ci sono scadenze per il mese di Febbraio***