Regolamento Europeo Privacy: Brevi note per capire cosa fare a partire dal 24 maggio 2018

Loris Beretta

ODCEC Milano

Le fonti normative

In data 15 dicembre 2015 è stato raggiunto a livello europeo un accordo per il nuovo Regolamento sulla Privacy o **GDPR** (General Data Protection Regulation). In conseguenza, per quanto riguarda l'Italia, l'abrogazione della direttiva 95/46/CE, c.d. "Direttiva Madre" comporterà la definitiva abrogazione del vigente D.Lgs. 196/2003.

Il 4 maggio 2016 è stata pubblicata sulla Gazzetta Ufficiale dell'Unione Europea la versione definitiva del testo del Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati; tale Regolamento è entrato in vigore il 25 maggio 2016 e si applica a tutti gli Stati Membri a partire dal 25 maggio 2018; entro tale termine tutti, aziende e professionisti, dovranno adeguarsi alla nuova legge sulla privacy. Ricordiamo che **i regolamenti UE sono immediatamente esecutivi,** non richiedendo la necessità di recepimento da parte degli Stati membri. Per questo motivo essi garantiscono una più efficace armonizzazione a livello europeo permettendo che la nuova normativa in tema di privacy entri contemporaneamente in vigore per tutti i ventisette stati membri UE.

Per l'Italia il Garante per la protezione dei dati continua e continuerà a rappresentare la fonte più attendibile per reperire documenti interpretativi e aggiornamenti sulle principali novità e linee guida.

Perchè

Dal 2003 ad oggi in qualità di titolari del trattamento dei dati ci siamo abituati a predisporre standard di richiesta di consenso, mentre come clienti e consumatori ci siamo abituati a firmare tali moduli pigramente senza neppure leggerli. Nel frattempo le tecnologie sono avanzate a velocità esponenziale determinando la messa in rete di miliardi di informazioni anche personali. Pensiamo ai social network alla tracciatura delle abitudini di acquisto da parte dei siti di vendita on-line, all'Internet of things che tra poco permetterà ad un semplice strumento, come ad esempio un orologio, di proporre la soluzione migliore per la soddisfazione di bisogni che ancora non ci siamo accorti di avere. Oggi lo sfruttamento delle informazioni è una nuova fonte di ricchezza e di potere, perciò è giusto che le autorità abbiano deciso di mettere ordine in questa materia prevedendo un sistema completamente nuovo di controlli, oneri e obblighi per chi raccoglie, utilizza e, magari, vende informazioni.

Cosa fare

Nonostante siano già passati due anni dall'entrata in vigore della nuova norma europea, tutto ciò è stato sino ad ora molto sottovalutato. Eppure, per Titolari e Responsabili del trattamento, le novità sono davvero tante. Innanzitutto viene introdotto il **principio della accountability** che comporterà l'onere di dimostrare

l'effettiva adozione di tutte le misure necessarie per il rispetto del Regolamento Europeo. Bisognerà redigere e conservare opportune documentazioni quali i **Registri delle attività di trattamento** (art. 30) in cui vengano riportate tutte le attività di trattamento dati svolte sotto la responsabilità del titolare al trattamento, o del responsabile (tale registro non è obbligatorio per tutti ma è altamente consigliabile la sua tenuta per dimostrare di aver messo in atto tutte le possibili azioni di messa in sicurezza dei dati ed evitare così le enormi sanzioni previste). Viene anche richiesto di cooperare con l'autorità di controllo notificando qualsiasi violazione dei dati personali alla stessa e al diretto interessato (art. 32-34).

Per questo si deve predisporre il **Privacy Impact Assessment**. Ossia diviene obbligatorio eseguire valutazioni d'impatto sulla protezione dei dati (art. 35), ed effettuare verifiche preliminari per diverse circostanze indicate da parte del Garante della Privacy.

Per noi italiani sicuramente tutto ciò è di difficile applicazione dato che siamo abituati a porre in essere comportamenti che in genere vengono precisamente codificati; questa volta, invece, la norma, dovendosi adattare a 28 paesi diversi, non poteva che disciplinare il tutto in via molto generale. Significa che sarà il titolare del responsabile del trattamento che dovrà decidere se e quali attività dovranno essere regolate dal GDPR e quali debbano essere le iniziative necessarie per renderle coerenti con la norma. Significa che per non rispondere di un danno commesso a causa di un certo trattamento di dati personali, occorrerà documentare, con il maggior dettaglio possibile, quali analisi dei processi sono stati compiuti e quali sono stati i provvedimenti messi in atto per evitare errori o problemi di qualsiasi genere. Infatti il GDPR all'articolo 25 viene definito "**data protection by default and by design**". Questo significa che la protezione dei dati deve essere il principale obiettivo di ogni progetto che preveda un qualsiasi trattamento di dati personali. Tutti i rischi per i diritti e le libertà degli interessati devono essere presi in grande considerazione fin dalla fase di progettazione di un processo, dell'erogazione di un servizio, della gestione di un sito, di un'iniziativa di marketing etc.. Il GDPR non è più un documento statico! Diventa un documento in continua evoluzione richiedendo un processo continuo di verifica e riadattamento al modificarsi delle procedure di raccolta, trattamento e finalità di gestione dei dati. Si potrebbe addirittura concettualmente parificare il GDPR al documento di valutazione dei rischi (DVR) in materia di sicurezza sul lavoro. Così quando un professionista, o un'impresa, presenta un preventivo non basterà più semplicemente che il cliente confermi l'accettazione del trattamento dei propri dati personali finalizzati all'erogazione del servizio. Il fornitore dovrà esprimere chiaramente che nella redazione del preventivo, nella definizione generale del servizio e nell'erogazione dello stesso esso pone in atto tutti i controlli e tutte le attività necessarie a garantire la tutela dei dati trattati.

Questa è la vera rivoluzione della nuova norma: non è più solo il cliente che accetta con qualche "crocetta" un certo tipo di trattamento dei propri dati personali ma è l'erogatore del servizio che deve dichiarare esplicitamente che i dati saranno convenientemente trattati e conservati con la massima garanzia di sicurezza grazie alle specifiche procedure adottate; dovranno essere esplicitati i diritti spettanti in tema di diritto di accesso, di opposizione al loro trattamento, di revoca del consenso in qualsiasi momento, notificando che, se del caso, è possibile presentare reclamo

all'autorità di controllo comunicando i dati necessari per farlo, il tutto nel modo più semplice e chiaro possibile. Si potrebbe quasi affermare che l'innovazione della norma porta a dire che la liceità del trattamento del dato supera l'importanza del consenso (che pur va necessariamente ottenuto).

Inoltre sarà necessario rendere una specifica formazione in tema di privacy che deve precedere l'accesso ai dati da parte di chi deve porre in essere il trattamento. Sostanzialmente significa che nessuno può accedere ai dati personali se non è istruito in tal senso dal titolare del trattamento. E si badi bene che la norma non parla di dipendenti e prescinde da qualsiasi tipo di rapporto di lavoro, questo significa che comprende qualsiasi soggetto interno o esterno allo studio o all'azienda che abbia, in qualsiasi modo, accesso ai dati. Occorre, dunque, stendere un vero e proprio piano di formazione approvato per iscritto dal titolare e dal responsabile del trattamento avvalendosi di docenti esperti specializzati in protezione dei dati personali. La formazione deve prevedere la somministrazione di un test di apprendimento al fine di poter dimostrare il raggiungimento degli obiettivi didattici e l'effettiva efficacia della formazione.

L'applicazione nel mondo del lavoro

Un particolare ambito nel quale appare particolarmente opportuno procedere alla "valutazione d'impatto" (Privacy Impact Assessment) è quello lavorativo. Basti pensare che i dipendenti, nelle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati" emanate il 4 aprile 2017, vengono definiti soggetti "vulnerabili". Sostanzialmente il contesto lavorativo è ritenuto rischioso per i diritti degli interessati considerato lo sbilanciamento di potere contrattuale a favore del datore di lavoro.

Il c.d. "Gruppo Articolo 29" (ossia il gruppo di lavoro istituito dall'art. 29 della direttiva 95/46 che già in passato aveva fornito indicazioni in materia di diritti dei lavoratori nell'ambito della protezione dei dati personali -opinion 8/2001 WP48 e WP55 del 2002-) dedica *l'opinion 2/2017* al tema del trattamento dei dati in ambito lavorativo commentando i nuovi obblighi introdotti dal Regolamento. In tale documento viene confermato che, anche quando si tratta di lavoro, ogni trattamento deve uniformarsi ai principi di trasparenza, necessità e minimizzazione del rischio. Viene ribadito che l'acquisizione del solo consenso non è un presupposto di legittimità sicuro e affidabile, posto che il lavoratore non può ritenersi completamente libero di acconsentire o di opporsi al trattamento in ragione della particolare relazione contrattuale che lo lega al datore di lavoro, trovandosi in una posizione di decisa sudditanza. Il Gruppo arriva a concludere che neppure la sola individuazione delle condizioni di legittimità del trattamento è sufficiente quando si tratta di controllo dei lavoratori. Occorre, pertanto, che i lavoratori siano anche compiutamente informati circa lo svolgimento delle attività di monitoraggio che su di loro incombono e per quali finalità vengono effettuate.

Anche l'internazionalizzazione delle imprese ha meritato l'attenzione del Gruppo che è giunto a stabilire che ogni trattamento effettuato all'interno di un gruppo imprenditoriale avente sedi in diversi Stati potrebbe comportare (o necessitare) il trasferimento di dati dei lavoratori e questo sarà legittimo solo a condizione che il

Paese terzo destinatario dei dati stessi assicuri un adeguato livello di protezione dei dati personali.

In sintesi, si può affermare che i principi di legittimità, trasparenza, proporzionalità, bilanciamento di interessi, minimizzazione dei rischi trovano piena applicazione anche in ambito lavorativo.

Per quanto riguarda l'Italia, poiché l'art. 88, 1° comma del Regolamento prevede che gli Stati membri possano dettare "*con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro*", potrebbe essere giunto il momento di mettere mano alla legge 20 maggio 1970, n. 300 ("Statuto dei Lavoratori") per valutare se sia ancora coerente con le nuove disposizioni, pur con le modifiche apportate dal Jobs Act, considerando anche le raccomandazioni del Gruppo di lavoro europeo, o se necessiti di qualche ulteriore adattamento.

Cosa manca

L'iter legislativo italiano in corso prevede un ultimo passo che dovrebbe concludersi entro il 21 maggio prossimo: l'approvazione definitiva del decreto di coordinamento con la normativa europea. Si tratta di un provvedimento già approvato in via preliminare dal Consiglio dei Ministri del 21 marzo 2018, in applicazione dell'articolo 13 della legge di delegazione europea 2016-2017 (legge 163/2017). In particolare, sarà stabilito il definitivo impianto sanzionatorio che è sicuramente il provvedimento più atteso da tutti gli operatori e saranno definiti i necessari adattamenti alle caratteristiche del nostro Paese.