MARCHESI MATTIOZZI
STUDIO LEGALE

IL NUOVO REGOLAMENTO UE 679/2016

09/03/2018

PANORAMICA

1. L'introduzione del GDPR

Il **25 maggio 2018** diviene operativo il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (allegato 1)

Tutti colo che trattano dati personali di persone fisiche in ambito UE sono soggetti al regolamento GDPR (General Data Protection Regulation), rimanendo escluse solo le autorità giudiziaria e la difesa.

2. Le novità

L'implementazione del GDPR richiede un **rinnovamento delle modalità e regole (policies) del trattamento dati da parte dei singoli imprenditori** che dovranno rivedere finalità, ambito, consistenza, modulistica, ruoli ecc. del loro trattamento dati.

Il Regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali (data breach).

L'informativa diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti.

Per facilitare la comprensione dei contenuti, nell'informativa si potrà fare ricorso anche a icone, identiche in tutta l'Unione europea. Gli interessati dovranno sapere se i loro dati sono trasmessi al di fuori dell'Ue e con quali garanzie; cosi come dovranno sapere che hanno il diritto di revocare il consenso a determinati trattamenti.

Il consenso dell'interessato al trattamento dei dati personali dovrà essere, come oggi, preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web).

Per trattare i dati sensibili, il Regolamento prevede che il **consenso deve essere anche «esplicito»**. Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate.

Il consenso potrà essere revocato in ogni momento. I trattamenti effettuati fino a quel momento dal titolare sulla base del consenso rimarranno comunque legittimi.

Con l'introduzione del cosiddetto **«diritto all'oblio»**, gli interessati potranno ottenere la cancellazione dei propri dati personali anche on line da parte del titolare del trattamento qualora ricorrano alcune condizioni previste dal Regolamento: se i dati sono trattati solo sulla base del consenso; se i dati non sono più necessari per gli scopi rispetto ai quali sono stati raccolti; se i dati sono trattati illecitamente; oppure se l'interessato si oppone legittimamente al loro trattamento.

A questo diritto si accompagna l'obbligo per il titolare del trattamento che ha pubblicato i dati di comunicare la richiesta di cancellazione a chiunque li stia trattando, nei limiti di quanto tecnicamente possibile.

Il diritto all'oblio potrà essere limitato solo in alcuni casi specifici: per esempio, per garantire l'esercizio della libertà di espressione o il diritto alla difesa in sede giudiziaria; per tutelare un interesse generale (ad esempio, la salute pubblica); oppure quando i dati, resi anonimi, sono necessari per la ricerca storica o per finalità statistiche o scientifiche.

Il titolare del trattamento dovrà **comunicare eventuali violazioni dei dati personali (data breach)** all'Autorità nazionale di protezione dei dati.

Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative. Il titolare del trattamento potrà decidere di non informare gli interessati se riterrà che la violazione non comporti un rischio elevato per i loro diritti (quando non si tratti, ad esempio, di frode, furto di identità, danno di immagine, ecc.); oppure se dimostrerà di avere adottato misure di sicurezza (come la cifratura) a tutela dei dati violati; oppure, infine, nell'eventualità in cui informare gli interessati potrebbe comportare uno sforzo sproporzionato (ad esempio, se il numero delle persone coinvolte è elevato). In questo ultimo caso, è comunque richiesta una comunicazione pubblica o adatta a raggiungere quanti più interessati possibile (ad esempio, tramite un'inserzione su un quotidiano o una comunicazione sul sito web del titolare).

L'Autorità di protezione dei dati potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria autonoma valutazione del rischio associato alla violazione.

Il Regolamento promuove la **responsabilizzazione (accountability) dei titolari del trattamento** e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

Il principio-chiave è «privacy by design», ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche.

Ad esempio, è previsto l'obbligo di effettuare **valutazioni di impatto prima di procedere ad un trattamento di dati** che presenti rischi elevati per i diritti delle persone, consultando l'Autorità di protezione dei dati in caso di dubbi.

Per il tipo di dati e di trattamento svolto può essere necessario adottare il **Registro delle attività di trattamento** previsto dall'art. 30 del GDPR, che potrà essere tenuto in modo informatico.

Viene inoltre introdotta la figura del **«Responsabile della protezione dei dati» (Data Protection Officer o DPO)**, incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti.

In compenso, scompaiono alcuni oneri amministrativi come l'obbligo di notificare particolari trattamenti, oppure di sottoporre a verifica preliminare dell'Autorità i trattamenti considerati «a rischio».

Il Regolamento promuove il ricorso a **codici di condotta** da parte di associazioni di categoria e altri soggetti, sottoposti all'approvazione dell'Autorità nazionale di protezione dei dati ed eventualmente della Commissione europea (nel caso dell'approvazione da parte della Commissione il codice di condotta avrà applicazione nell'intera Ue).

Il titolare potrà far certificare i propri trattamenti, in misura parziale o totale, anche ai fini di trasferimenti di dati in Paesi terzi.

La certificazione potrà essere rilasciata da un soggetto abilitato oppure dall'Autorità di protezione dei dati. L'adesione ai codici di condotta e la certificazione del trattamento saranno elementi di cui l'Autorità dovrà tenere conto, per esempio, nell'applicare eventuali sanzioni o nell'analizzare la correttezza di una valutazione di impatto effettuata dal titolare.

3. Cosa si dovrà fare

L'adeguamento al GDPR sarà complicato ed oneroso per gli imprenditori che dovranno, quanto meno:

A. Ridefinire tipo e consistenza dei dati trattati, indicando le finalità e la necessità
B. Definire i ruoli del titolare del trattamento dei dati (in ipotesi Legale rappresentante), individuare ruoli e funzioni di eventuali "responsabili" per il trattamento dei dati e, opportuno ma non obbligatorio, delegare specifiche funzioni agli "incaricati".
C. Eventualmente, o necessariamente ricorrendone i presupposti, nominare un Responsabile della Protezione dei Dati (RPD o in inglese DPO Data Protection Officer), una figura autonoma e con potere decisionale e di spesa che si rapporta solo con i vertici dell'Ente.
D. Riformulare la modulistica relativa alle informative, ai consensi, ai reclami, al diritto di accesso ai dati, privilegiando le modalità telematiche.
E. Adottare, ove previsto, il Registro delle attività di trattamento, preferibilmente in forma elettronica.
F. Rivedere e/o adottare misure per la sicurezza dei dati, in specie per il sistema informatico, con strategie di archiviazione, conservazione a norma e disaster recovery.
G. Effettuare una Valutazione di impatto sulla protezione dei dati (assessment – art. 35 GDPR)
H. Adottare codici di condotta (e/o certificazioni, quando saranno disponibili e definite le relative autorità).

4. Opportunità

È chiaro che l'adeguamento al GDPR comporterà un costo per le aziende, in termini di tempo e lavoro per effettuare i processi di analisi, implementazione, formazione e manutenzione ed in termini di consulenza esterna. Ma può essere anche l'occasione per ripensare ed integrare i processi amministrativi e di gestione dei dati e del ciclo di fatturazione.

Molte delle attività ed adempimenti descritti nel paragrafo precedente ben si prestano ad essere trattate o adempiute con implementazione informatica. Si può individuare un'impresa che offra il servizio di Valutazione d'impatto (Assessment) e/o di verifica della sicurezza dei sistemi informatici a costi convenzionati.

Infine, citiamo le parole di Google sul tema:

"*Dovresti inoltre rivolgerti a consulenti legali indipendenti per conoscere il tuo stato e gli obblighi previsti dal regolamento GDPR, dato che solo un avvocato può fornire informazioni legali specifiche per la tua situazione. Tieni presente che le informazioni in questo sito web non forniscono indicazioni legali né sostituiscono la consulenza di un avvocato*."

(https://www.google.com/intl/it/cloud/security/gdpr/)

MARCHESI MATTIOZZI
STUDIO LEGALE

Per maggiori informazioni, senza impegno, contatta lo Studio Legale dell'avv. Giulio Marchesi.

24122-I Bergamo, via Duca degli Abruzzi 5, tel. 035223040 fax 0356305249, email: info@avvocatomarchesi.it - www.giulio-marchesi.com.

"let's overcome the obstacles together!"