Privacy

Protezione dei dati personali: tra definitiva applicabilità del GDPR e attesa del decreto attuativo

8 maggio 2018

Come noto, in data 14 aprile 2016 il Parlamento Europeo ha approvato il nuovo regolamento in materia di protezione dei dati personali (Regolamento 2016/679 – *General Data Protection Regulation "GDPR"*).

Il regolamento, che ha abrogato la Direttiva 95/46/Ce, sebbene in vigore, prevede che divenga pienamente applicabile solo a decorrere dal 25 maggio 2018. In realtà, sono poche le imprese che hanno effettivamente sfruttato il periodo concesso per avviare un graduale processo di adeguamento e risultare *compliant* alla scadenza del 25 maggio.

Solamente negli ultimi mesi infatti le imprese, riconosciuta l'imminenza della scadenza, hanno iniziato a muoversi per raggiungere l'obiettivo della conformità al GDPR. D'altra parte il processo di adeguamento, soprattutto per imprese di grandi dimensioni e/o che trattano categorie particolari di dati personali (i dati in precedenza definiti "dati sensibili"), risulta tutt'altro che agevole, ed è per questo che molti hanno deciso di farsi assistere da consulenti legali e IT per essere meglio guidate lungo la strada della *compliance*.

Il Regolamento come opportunità di miglioramento per le imprese

L'attività di adeguamento non deve essere realizzata considerando il GDPR come una mera prescrizione volta ad appesantire il lavoro delle imprese rallentandone e limitandone lo svolgimento delle attività.
La protezione dei dati personali infatti non costituisce un vincolo che irrigidisce i processi in una rete di adempimenti formali, ma al contrario si configura come un valido strumento di aiuto per la semplificazione dei processi.
Avere conoscenza dei processi esistenti ed elaborare specifiche procedure operative per mette ad ogni persona operante all'interno dell'impresa di acquisire maggiore consapevolezza su come gestire le situazioni ordinarie e, soprattutto, straordinarie.

In secondo luogo, non bisogna dimenticare che la protezione dei dati personali nasce prima di tutto come diritto dell'interessato.
Tale diritto comprende non solo la protezione dei dati contro potenziali minacce esterne (es. furto di dati), ma anche e soprattutto il diritto al pieno controllo sui propri dati. Assicurare la protezione dei dati personali non significa quindi blindare i dati in modo da renderli non accessibili a soggetti diversi dall'interessato (procedendo lungo questa via si finirebbe per penalizzare l'interessato precludendogli la possibilità di usufruire di una pluralità di servizi).
Scopo del diritto alla privacy è, all'opposto, agevolare la fruizione di servizi che implicano un trattamento di dati

personali garantendo, a chiunque decida di accedervi, la possibilità di mantenere il controllo sui propri dati. Un soggetto consapevole delle modalità e delle finalità di utilizzo dei propri dati avrà, d'altra parte, una maggiore disponibilità a fornirli e, di conseguenza, a rivolgersi ad un'impresa.

Non meno importante è poi l'introduzione da parte del GDPR di sanzioni amministrative e penali particolarmente severe. L'art. 83 GDPR prevede infatti, in caso di violazioni, sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo, se superiore.

I principi ispiratori del Regolamento

Rispetto alla precedente disciplina privacy, dettata in Italia dal Codice sulla protezione dei dati personali (d.lgs. 196/2003), il Regolamento UE introduce una nuova prospettiva: piuttosto che dettare regole specifiche che irrigidiscono il sistema e, nella maggior parte dei casi, rischiano di rimanere mere prescrizioni formali, si preferisce adottare un sistema flessibile che possa essere adeguato al contesto specifico di ogni impresa. Principio cardine del GDPR è infatti la c.d. *accountability* (responsabilizzazione), secondo cui non sono previste misure obbligatorie la cui applicazione è necessaria e sufficiente a garantire la conformità alla normativa; è posto però in capo al titolare del trattamento l'onere di adottare tutte le misure che, in relazione allo stato dell'arte, alla tipologia di dati trattati e al rischio esistente per i diritti e le libertà dell'interessato, possano garantire una effettiva tutela dei dati personali trattati.

Altro importante principio introdotto dal GDPR è quello della *privacy by design* e *privacy by default*. Esso si fonda sull'idea che un atteggiamento di prevenzione *ex ante* sia più efficace di un intervento riparatorio *ex post*: piuttosto che porre rimedio a una violazione già avvenuta, è necessario intervenire nella fase di ideazione dei processi. Il tema della protezione dei dati personali deve essere quindi affrontato fin dalla fase di progettazione: tutti i processi di trattamento devono essere elaborati prevedendo modalità tali da garantire sin dall'inizio che i dati siano trattati nel rispetto della disciplina e adottando "di default" impostazioni che ne minimizzino l'uso.

Il processo di adeguamento: attività da svolgere

Nell'ottica del GDPR le imprese, per poter arrivare ad essere *compliant*, dovranno analizzare i propri processi, trattamento per trattamento, e, sulla base di una adeguata valutazione dei rischi che essi comportano, adottare idonee misure di garanzia.
Secondo la nostra esperienza, un efficace processo di adeguamento deve necessariamente comprendere una pluralità di fasi, più o meno articolate a seconda delle dimensioni dell'impresa.
Tra le attività principali rientrano:

- verifica "*as is*" attraverso l'individuazione dei trattamenti esistenti e l'analisi e mappatura dei processi interni;
- *gap analysis*, ovvero l'individuazione e la presa d'atto delle criticità attualmente esistenti;
- definizione delle misure organizzative, tecniche e di sicurezza da implementare;

- predisposizione di un registro dei trattamenti, ove opportuno;
- valutazione della opportunità / necessità di nominare un DPO (Data Protection Officer – responsabile della protezione dei dati);
- valutazione della opportunità/necessità di svolgimento di una DPIA (Data Protection Impact Assessment – Valutazione d'impatto sulla protezione dei dati).

Decreto legislativo per l'adeguamento della normativa nazionale alle disposizioni del GDPR: possibili novità in ambito sanitario.

Da ultimo si segnala che è in fase di approvazione il decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR.
Lo schema di decreto prevede l'abrogazione del Codice privacy che sarà quindi interamente sostituito dal regolamento, salve le integrazioni introdotte dal decreto stesso.
Al riguardo si segnalano, ad esempio, importanti novità in relazione al trattamento di dati relativi alla salute per finalità di cura da parte degli organismi sanitari italiani che – sulla base dello schema di decreto attuativo circolato informalmente – potrà avvenire in assenza del preventivo consenso espresso da parte del paziente interessato.
Il quadro normativo in materia di protezione dei dati personali è quindi profondamente cambiato e, considerate anche le sanzioni previste dal GDPR, è senz'altro opportuno che tutti i soggetti coinvolti avviino senza ulteriori ritardi le attività di adeguamento al fine di garantire la conformità.

Ughi e Nunziante – Studio Legale