FANTIGROSSI
dal 1984
STUDIO LEGALE

Il nuovo Regolamento europeo in materia di protezione dei dati personali: 25 maggio 2018 una scadenza da affrontare subito.

1. Le linee generali del regolamento e l'ambito di applicazione

A decorrere dal **25 maggio 2018**, in tutti gli **Stati membri dell'UE** sarà applicabile il nuovo Regolamento **GDPR** (*General Data Protection Regulation*) – **UE 2016/679**, in materia di protezione dei dati personali, che sostituisce la precedente Direttiva 95/46 e ogni disposizione nazionale con essa non compatibile.

Si tratta di una scadenza apparentemente lontana, ma che in realtà richiede che il processo di adeguamento inizi per tempo. Scopo di queste note è quello di dare una visione introduttiva e d'insieme dei contenuti del Regolamento e di evidenziare le prime tappe di questo percorso.

Va tenuto presente in primo luogo il criterio di applicabilità territoriale del Regolamento: la relativa disciplina riguarda ogni trattamento dei dati personali di soggetti stabiliti nel territorio UE, anche qualora il soggetto titolare del trattamento sia stabilito in un Paese extra UE.

La normativa avrà quindi come destinatari anche i numerosi fornitori di *Internet service providing* stabiliti all'estero.

Quanto al profilo soggettivo, i principali destinatari degli obblighi connessi alla tutela dei dati personali sono **imprenditori, società, enti pubblici, associazioni e liberi professionisti.**

Il Regolamento, facendo perno sul concetto di ***accountability*** ("responsabilizzazione"), mira alla creazione di un sistema uniforme improntato alla neutralizzazione di ogni possibile rischio connesso al trattamento; tale scopo è perseguito imponendo ai **titolari e ai responsabili del trattamento dei dati** di individuare i rischi connessi all'attività di trattamento e adottare idonee misure di prevenzione degli stessi.

> La creazione di un modello di prevenzione del rischio effettivamente conforme alle prescrizioni del Regolamento è di particolare importanza, dal momento che la responsabilità del titolare e del responsabile del trattamento, in sede di comminazione delle ingenti sanzioni previste, sarà valutata dall'Autorità di controllo in relazione alla capacità che questi avranno di **dimostrare di aver adottato ogni misura necessaria per garantire la sicurezza dei dati trattati**, in conformità alle previsioni del regolamento stesso (art. 24).

20122 MILANO - Corso Italia, 7 - tel. +39 02 86450084 +39 02 86990734 - fax. +39 02 867613
29121 PIACENZA - Largo Matteotti, 7 - tel. +39 0523 336694
mail. studiolegale@fantigrossi.it - web. www.fantigrossi.it

In sostanza in relazione ai trattamenti di dati personali opera una presunzione di responsabilità in capo a chi li effettua: in caso di eventi dannosi spetterà a lui e non al danneggiato provare di aver operato correttamente.

Naturalmente i cambiamenti più radicali interesseranno in particolare quei soggetti destinatari di obblighi specifici, come gli enti pubblici e le società che trattano dati sensibili o effettuano regolarmente attività di profilazione, per le quali si imporrà la nomina di un *data protection officer*, figura di nuova introduzione di cui si dirà nel prosieguo.

In generale, si va incontro ad un nuovo modello di *gestione e controllo dei dati* che richiede più consapevolezza, una professionalità specifica (con figure interne o esterne) ed un continuo aggiornamento.

2. La valutazione dei rischi e le misure preventive

Il concetto portante che anima la riforma è quello di **"*data protection by default and by design*"** contenuto nell'art. 25. In base a tale principio, i titolari e i responsabili del trattamento dovranno poter garantire la sicurezza dei dati trattati attraverso l'adozione di un sistema idoneo a prevenire violazioni degli stessi in ogni fase del trattamento.

La particolarità consiste nel fatto che tale sistema dovrà essere **concepito e realizzato sin da subito**, in via preliminare rispetto all'esercizio dell'attività di trattamento vera e propria, intraprendendo azioni specifiche e dimostrabili.

A tale scopo, sarà necessario effettuare una **analisi preventiva del rischio** inerente al trattamento (artt. 35-36); tale analisi consiste nel rilevamento di ogni possibile **impatto negativo su libertà e diritti degli interessati** cui è esposta l'attività di trattamento dati e la specifica individuazione delle misure necessarie a neutralizzare questo rischio.

Il Regolamento lascia peraltro una relativa **autonomia ai titolari e ai responsabili quanto alle concrete misure da adottare**, ponendo piuttosto un "vincolo di risultato"; l'idoneità delle misure sarà infatti valutato in relazione alla loro capacità di: "garantire un livello di sicurezza adeguato al rischio" (art. 32).
L'art. 32 fornisce comunque un elenco di alcune "misure tipo", da intendersi, tuttavia, come non tassative e meramente esemplificative, come la pseudonimizzazione e la cifratura dei dati,.

Il rispetto da parte del titolare del trattamento degli obblighi posti dal Regolamento dovrà **poter essere dimostrato**. Il Regolamento stesso indica strumenti utili a tal fine, quali l'adesione a **codici di condotta** e **meccanismi di certificazione** (artt. 40 e 42).

3. Gli obblighi di comunicazione e notifica

Individuati i rischi e adottate le misure di prevenzione, i titolari decideranno **in autonomia** di iniziare l'attività di trattamento. **Non sarà più necessaria difatti la previa notifica all'Autorità di controllo**, sino ad ora finalizzata ad una verifica *ex ante* circa i presupposti del trattamento; ciò non di meno, l'Autorità è investita di significativi poteri di indagine e verifica *ex post* sull'idoneità delle misure prescelte dall'operatore, fino all'indicazione di eventuali correttivi da applicare (art. 58, comma 2).

Il Regolamento prevede **tuttavia due ordini di comunicazioni** che vanno, in alcuni casi, **obbligatoriamente effettuate** dal titolare nelle **ipotesi in cui si verifichi una violazione** dei dati personali ("**data breach"**).

La prima è prevista dall'art. 33 e consiste in una notifica, da fare **all'Autorità di controllo,** di ogni violazione di cui il titolare venga a conoscenza, qualora la violazione "presenti un rischio per i diritti e le libertà delle persone fisiche". Tale comunicazione dovrà essere data entro 72 ore e, comunque, "senza ingiustificato ritardo".

La seconda è prevista dall'art. 34 e prevede, nei casi di violazioni più gravi, che il titolare effettui una **comunicazione allo stesso interessato**. Questo secondo ordine di comunicazione è all'evidenza il più delicato, attese le possibili ripercussioni negative sulla reputazione della società che conserva i dati; il Regolamento ha perciò inteso mitigare l'obbligo di comunicazione all'interessato, escludendolo nei casi in cui il titolare dimostri di essersi adoperato adeguatamente per adottare tutte le misure necessarie a proteggere i dati violati e, in seguito alla violazione, abbia operato efficacemente per limitarne le conseguenze.

4. Il Responsabile della protezione dei dati (RPD)

Altra fondamentale innovazione è rappresentata dall'introduzione della figura del responsabile per la protezione dati (RPD), comunemente noto con l'acronimo inglese (DPO) (Data Protection Officicers).

Tale figura sarà obbligatoria per tutte le **autorità pubbliche e organismi pubblici** (ad eccezione delle autorità giurisdizionali), per i **soggetti privati che svolgano regolare attività di monitoraggio** di dati personali (rientrano pacificamente in tale categoria tutti quei soggetti che svolgono attività di profilazione, anche a scopi commerciali) e per i soggetti che trattano regolarmente flussi di **dati sensibili**, come quelli relativi a condanne penali o a condizioni di salute dei pazienti in cura presso aziende ospedaliere.

Il RPD potrà svolgere le sue funzioni sia da dipendente che nell'ambito un rapporto di consulenza esterna: l'importante è che operi in modo del tutto indipendente. È difatti richiesto che chi ricopre questo ruolo non versi in situazione di conflitto di interessi rispetto ad altre funzioni a lui affidate e che non vi sia alcuna ingerenza del titolare o del responsabile del trattamento nella definizione dei compiti di monitoraggio e supervisione; dovrà poi poter accedere

in totale autonomia e in qualsiasi momento ai dati, e intraprendere tutte le azioni che ritenga più opportune per garantirne la sicurezza.

Il RPD sarà investito, in particolare, di funzioni di sorveglianza sull'osservanza del Regolamento e di consulenza al titolare sulle opportune misure di sicurezza da adottare, in modo da poter essere il referente per i rapporti con l'Autorità di controllo. A tal fine, è importante che sia adeguatamente coinvolto in ogni questione riguardante la protezione dei dati e costantemente aggiornato su ogni aspetto del trattamento, in modo da poter effettuare un costante monitoraggio.

Il Regolamento non detta disposizioni di dettaglio sulle particolari qualifiche del DPO, ma stabilisce che questo sia designato in funzione delle sue qualità professionali, che devono essere adeguate alle mansioni svolte. Sarà ovviamente necessaria una approfondita conoscenza del Regolamento e di tutta la normativa e prassi in tema di privacy e protezione dei dati, unita ad una idonea preparazione tecnico-informatica; in rapportato alla complessità del settore di riferimento. Non è comunque richiesto il possesso di abilitazioni o attestazioni formali, né è prevista l'istituzione di un apposito albo professionale per tali figure.

5. Il registro dei trattamenti.

In coerenza con l'obiettivo di costante monitoraggio del rischio e allo scopo di agevolare i controlli del Garante nella fase del trattamento, il Regolamento prevede l'obbligo di tenuta di un registro dei trattamenti che contenga la descrizione di tutte le operazioni svolte (art. 30).

Il registro dovrà essere tenuto in forma scritta, anche elettronica, ed è obbligatorio per tutti i titolari e i responsabili del trattamento; l'unica esenzione è prevista per gli organismi con meno di 250 dipendenti, nel caso in cui questi non effettuino trattamenti a rischio (art. 30, par. 5).

Il regolare aggiornamento del registro gioca un ruolo fondamentale nel descritto contesto normativo che, come visto, attribuisce al titolare del trattamento una forte autonomia quanto alla valutazione del rischio; esso fa quindi da contraltare al venire meno dell'obbligo di notifica preventiva del trattamento all'Autorità di controllo, agevolando le operazioni di verifica in fase di svolgimento dell'attività.

6. Note conclusive.

Le sanzioni previste in caso di violazioni del Regolamento sono particolarmente elevate, potendo arrivare per le imprese fino al 4% del fatturato annuo.

Occorre quindi sottolineare, in conclusione, l'importanza che rivestirà la capacità delle società di munirsi di un sistema di prevenzione efficace; il regolamento prevede infatti che, nel determinare gli importi delle sanzioni da comminare,

l'Autorità di controllo effettui una valutazione del grado di responsabilità del titolare del trattamento e del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto e delle misure adottate per attenuare il danno subito dagli interessati, nonché del grado di cooperazione con l'Autorità di controllo.

La migliore prevenzione al riguardo è quella che passa attraverso un percorso di formazione interna, di analisi dell'impatto della disciplina della privacy nella specifica realtà aziendale o dell'ente e di individuazione di figure di riferimento professionalmente adeguate.

Milano, ottobre 2017

(avv. Umberto Fantigrossi) (avv. Valeria Fantigrossi)