Privacy

Il Nuovo Regolamento Generale sulla Protezione dei Dati

5 maggio 2016

Lo scorso 27 aprile 2016 il Parlamento Europeo ha approvato il regolamento (2016/679) che uniformerà e rinnoverà la disciplina in materia di protezione di dati personali applicabile in tutti i paesi dell'Unione Europea. Il testo è stato pubblicato nella gazzetta ufficiale dell'Unione Europea il 4 maggio 2016 e dovrà essere implementato progressivamente nei prossimi due anni

Ambito di applicazione

Una prima importante novità riguarda l'ambito di applicazione del regolamento. Infatti, recependo la giurisprudenza della Corte di Giustizia (cfr. cd. caso Google Spain C-131/12), le nuove norme si applicheranno ai trattamenti di dati personali che saranno effettuati da titolari del trattamento o da responsabili stabiliti nel territorio dell'Unione anche se compiuti al di fuori dell'Unione nonché ai trattamenti svolti da soggetti non stabiliti nel territorio dell'UE, quando le relative attività siano finalizzate all'offerta di beni e servizi nell'Unione o al controllo del comportamento di interessati che si trovino nel territorio europeo.

I principi

L'impianto dei principi ispiratori della direttiva 95/46/CE sulla privacy è al tempo stesso confermato ed esteso dal Regolamento. Tra le novità, si segnala l'introduzione del principio di trasparenza; e di quello di *accountability*, strettamente legato all'onere di provare, in ogni momento, di aver adottato tutte le misure atte a garantire la *compliance* al regolamento.

I diritti

Anche i diritti dell'interessato risultano ampliati. Da un lato, viene espressamente disciplinato il diritto all'oblio, e, dall'altro, si introduce il diritto alla portabilità dei dati - un'assoluta novità - che attribuisce all'interessato la facoltà di richiedere al titolare del trattamento che siano trasferiti a lui, o a terzi, i dati personali in suo possesso in un formato strutturato, di uso comune e leggibile.

I doveri del titolare del trattamento

Rispetto alle previsioni della Direttiva 95/46/CE, viene esteso il contenuto obbligatorio della informativa che deve essere fornita agli interessati. I titolari del trattamento dovranno inoltre strutturare la propria attività al fine di assicurare che - di *default* - siano oggetto di trattamento i soli dati necessari (in termini di quantità, accessibilità e tempi di conservazione dei dati raccolti e di estensione del trattamento) per ogni specifica attività del trattamento (cd. *privacy by default*).

Allo stesso modo, sin dalla fase di progettazione e sviluppo di un nuovo servizio o prodotto e di una modalità di trattamento, il responsabile del trattamento dovrà mettere in atto misure tecniche e organizzative tali da garantire un'adeguata *compliance* alle prescrizioni del regolamento (cd. *privacy by design*).

Un'altra importante novità riguarda l'obbligo del titolare del trattamento di notificare al Garante eventuali violazioni dei dati personali realizzate da soggetti non autorizzati (*data breach*) e, in presenza di determinate circostanze, di estendere tale notificazione anche all'interessato. Ancora, ogni qual volta il trattamento avvenga attraverso nuove

tecnologie e sussista un rischio significativo per i diritti e per le libertà degli interessati, il titolare del trattamento dovrà effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali e, nei casi in cui sia riscontrato un rischio elevato, per l'individuazione di adeguate contromisure da parte del titolare del trattamento dovrà essere interpellata l'Autorità Garante.
Infine, nelle ipotesi in cui il trattamento sia svolto da un ente pubblico, oppure sia fatto utilizzo di dati su larga scala o siano trattati dati sensibili o giudiziari, il titolare del trattamento dovrà designare una nuova figura, il **Data Protection Officer**. Questa nuova figura è denominata, nella versione italiana del regolamento, "Responsabile della Protezione dei Dati" ma non va confusa con la figura tradizionale del "Responsabile del trattamento dei dati" (*data processor*). Infatti, mentre quest'ultimo risponde al titolare per il proprio operato, al *Data Protection Officer* dovrà essere garantita autonomia e indipendenza, e avrà numerosi compiti informativi, consultivi, di cooperazione ed interazione con l'autorità di vigilanza.
Il *Data Protection Officer* può essere esterno all'organizzazione del titolare oppure anche essere un dipendente del titolare o del responsabile del trattamento, purché però gli siano assicurate le menzionate autonomia ed indipendenza.

Trasferimento Dati all'Estero
Le modalità di trasferimento dei dati in paesi extra-UE vengono rimaneggiate. Rimane il principio della libera circolazione dei dati nel territorio dell'Unione e verso Paesi extra-europei oggetto di apposite decisioni di adeguatezza da parte della Commissione. Allo stesso modo, salvo il consenso dell'interessato, il trasferimento in paesi extra-UE sarà legittimo solo nel caso in cui il soggetto che intende effettuarlo presti idonee garanzie. Tuttavia, il procedimento di deliberazione della Commissione è stato rivisto e sono stati ampliati gli strumenti tramite cui fornire le necessarie garanzie.

Le Autorità Garanti
Anche la composizione di ruoli e competenze delle Autorità Garanti degli Stati membri risulta ridisegnata. La principale novità è la realizzazione del sistema del c.d. "sportello unico". I cittadini potranno rivolgersi ad una sola Autorità Garante in caso di violazioni da parte di imprese multinazionali e, al contrario, le aziende potranno fare riferimento ad una sola Autorità, quella del paese in cui ha sede lo stabilimento principale.
È stato poi istituito il Comitato Europeo per la Protezione dei Dati che avrà principalmente una funzione di armonizzazione della applicazione del Regolamento tramite l'adozione di linee guida, studi, raccomandazioni e *best practice*.

Sanzioni e Tutele
La riforma, infine, incide sensibilmente sull'impianto sanzionatorio. Al riguardo, si segnala in particolare il significativo inasprimento delle sanzioni amministrative che potranno essere comminate dalle autorità garanti dei paesi membri.
A titolo esemplificativo, si consideri che per le violazioni delle disposizioni in materia di *privacy by default* o nei casi di mancata notifica di *data breach* o di mancata effettuazione della valutazione di impatto, sono previste sanzioni fino a 10 milioni di Euro o, in alternativa, nel caso in cui il soggetto che abbia commesso la violazione sia un'impresa, fino al 2% del fatturato globale annuo, se maggiore.

Sanzioni ancor più elevate (fino ad un massimo di 20 milioni di Euro o fino al 4% del fatturato mondiale annuo dell'impresa) sono invece previste per violazioni quali l'omessa o inidonea informativa o per trasferimenti di dati a paesi terzi effettuati in violazioni delle previsioni del Regolamento.

Ughi e Nunziante – Studio legale