

Il Regolamento Europeo N. 2016/679

A cura degli avv.ti Simona Cardillo e Daniela Cardillo

**LA NUOVA DISCIPLINA SULLA PRIVACY**

**LA NUOVA DISCIPLINA SULLA PRIVACY. IL REGOLAMENTO EUROPEO N. 2016/679**

Dopo un *iter* legislativo durato quattro anni, il 14 aprile 2016 è stato approvato dal Parlamento Europeo il Regolamento n. 2016/679 “*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*” che, pubblicato in Gazzetta Ufficiale UE il 4 maggio 2016 ed entrato in vigore 20 giorni dopo, diventerà definitivamente applicabile in tutti i Paesi dell’Unione Europea a partire dal 25 maggio 2018 così sostituendo, in Italia, il Codice della Privacy (D.lgs. n. 196/2003).

La nuova normativa mira ad adeguare la *data protection* all’evoluzione tecnologica che ha determinato un aumento dei flussi transfrontalieri e quindi dei dati scambiati, con l’obiettivo, da un lato, di agevolare la libera circolazione di dati all’interno dell’UE e, dall’altro lato, di garantire un più elevato livello di protezione.

Una delle caratteristiche più innovative e di maggior rilievo del Regolamento n. 2016/679 consiste sicuramente nel suo ambito di applicazione in quanto è stata sancita una sostanziale extra-territorialità dell’efficacia del Regolamento.

Il Regolamento sarà, infatti, applicabile non solo ai casi in cui il soggetto che tratta i dati (sia esso il Titolare o il Responsabile del trattamento) sia stabilito nell’Unione ma anche ai casi in cui il soggetto cui i dati personali si riferiscono si trovi sul territorio europeo purchè il trattamento riguardi l’offerta di beni e/o servizi oppure riguardi il monitoraggio del comportamento dell’interessato all’interno dell’Unione Europea.

Il Regolamento Europeo introduce molte altre novità, alcuni istituti già presenti sotto il vigore del Codice della Privacy vengono estesi nella loro applicazione, la tutela di alcuni diritti viene intensificata ed alcuni adempimenti vengono abrogati.

In particolare, come ben rappresentato dall’abrogazione della preventiva notificazione dei trattamenti al Garante, sono destinati a snellirsi gli adempimenti formali e, seppure il profilo burocratico non venga meno del tutto, si può ritenere che il cuore della nuova disciplina sia improntato all’instaurazione di tutele sostanziali.

Il regolamento prevede, infatti, fra i suoi pilastri il principio di *accountability* (termine che, ai fini della normativa in commento, racchiude i significati di *responsabilizzazione* e di *obbligo di rendicontazione*) che riguarda tutti i soggetti e che impone ai Titolari ed ai Responsabili di adottare un comportamento proattivo e tale da dimostrare la concreta adozione di misure finalizzate ad assicurare la conformità delle attività di trattamento alle disposizioni del Regolamento. Non vengono specificati i comportamenti, viene invece affidato ai Titolari il compito di decidere autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Il citato principio di *accountability* sancisce il salto di qualità nei sistemi di gestione dei dati ossia il passaggio da una concezione prettamente formale di mero adempimento ad un approccio, appunto, sostanziale di tutela dei dati e delle persone stesse ed è pertanto strettamente connesso con le misure di sicurezza, con l’analisi del rischio, con la valutazione di impatto *privacy* e con i principi di *Privacy by design* e *Privacy by default* (di cui si dirà brevemente) che devono essere presenti nella progettazione di servizi e programmi.

La valutazione dell’impatto *privacy* (*c.d.* PIA o *Privacy Impact Assessment)* ai sensi dell’art. 35 dovrà essere effettuata quando un determinato trattamento - tenuto conto dell’uso di nuove tecnologie e della sua natura, del contesto e delle finalità - possa presentare un rischio elevato per i diritti e per le libertà delle persone fisiche e costituirà la base su cui costruire l’intero sistema di misure idonee di sicurezza.

Il Responsabile e il Titolare dovranno inoltre tenere un registro delle attività di trattamento in forma scritta, anche in formato elettronico, contenente gli elementi di cui all’art. 30 del Regolamento. L’obbligo di tenuta del registro non si applicherà tuttavia, in linea di principio, alle imprese e alle organizzazioni con meno di 250 dipendenti (con limitate eccezioni).

Nel nuovo Regolamento un’intera sezione è poi dedicata alla Trasparenza (Sezione 1 del Capo III) la quale richiede, con riferimento alle modalità di trattamento dei dati, che le informazioni all’interessato:

1. siano rese con un linguaggio semplice e chiaro, soprattutto nel caso di minori;

(ii) abbiano sempre forma scritta, essendo ammessa l’informativa orale solo quando ciò è richiesto dall’interessato e l’identità di questi possa essere provata con altri mezzi;

(iii) prevedano, *inter alia*, il periodo di conservazione dei dati personali, il diritto di proporre reclamo ad un’autorità di controllo e l’eventuale intenzione del Titolare di trasferire dati personali ad un Paese terzo.

Altri due principi di particolare rilievo sono costituiti, come si è accennato, dalla *c.d.* *Privacy by design*, cheimpone al Titolare di adottare e attuare misure tecniche e organizzative che tutelino i principi di protezione dei dati sin dal momento della progettazione oltre che nell’esecuzione del trattamento e dalla *c.d. Privacy by default* la quale indica la necessità di adottare, come modalità operativa del trattamento, misure e tecniche che, per impostazione predefinita, garantiscano l’utilizzo dei soli dati personali necessari per ciascuna specifica finalità di trattamento.

Inoltre, vengono intensificati alcuni diritti già esistenti, quali il diritto all’oblio e il diritto alla portabilità dei dati, e viene introdotta una figura professionale nuova, il Responsabile della Protezione dei Dati (*c.d.* DPO, *Data Protection Officer*), il quale dovrà essere obbligatoriamente nominato nelle aziende pubbliche e in quelle impegnate nel trattamento di dati personali su larga scala. Tale figura sarà caratterizzata da una posizione di autonomia e indipendenza ed avrà la responsabilità di un ufficio *privacy* a garanzia della correttezza dei trattamenti.

In merito al *Data breach*, mentre attualmente è previsto che solo i “*fornitori di servizi di comunicazione elettronica accessibili al pubblico*” abbiano l’obbligo di comunicare l’avvenuta violazione di dati personali al Garante per la protezione dei dati personali e, in determinati casi, anche al contraente/cliente, il Nuovo Regolamento estende tale obbligo di comunicazione a tutti i Titolari e i Responsabili, quali che siano i trattamenti posti in essere (artt. 33 e 34).

Nello specifico, il Responsabile dovrà informare il Titolare della violazione senza ingiustificato ritardo e quest’ultimo dovrà notificare la violazione, a sua volta senza ingiustificato ritardo e, possibilmente, entro 72 ore dal momento in cui ne sarà venuto a conoscenza, all’autorità di controllo (*i.e*. al Garante), a meno che sia improbabile che tale violazione presenti rischi per i diritti e le libertà delle persone.

In caso di violazione suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche sarà inoltre d’obbligo effettuare la comunicazione anche all’interessato.

Con riferimento al sistema sanzionatorio introdotto dalla nuova disciplina, si consideri che chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento avrà il diritto di ottenere il risarcimento del danno da parte del Titolare o del Responsabile del trattamento. Le azioni legali per l’esercizio di tale diritto dovranno essere promosse innanzi alle autorità competenti a norma del diritto dello Stato membro e, per l’Italia in particolare, avanti al Tribunale Ordinario.

Il Titolare ed il Responsabile del trattamento, per essere esonerati da responsabilità, dovranno dimostrare che l’evento dannoso non è loro in alcun modo imputabile. Sotto il regime del Regolamento si attuerà, in altri termini, un’inversione dell’onere della prova.

Ai sensi dell’art. 83 del Regolamento, le sanzioni amministrative pecuniarie potranno spingersi, in base alle violazioni commesse, sino ad € 10.0000.000,00 o al 2% del fatturato mondiale totale annuo dell’esercizio precedente se superiore, oppure, per le infrazioni più gravi, sino ad € 20.0000.000,00 o fino al 4% del fatturato mondiale totale annuo dell’esercizio precedente se superiore.

Si rileva infine che il Legislatore europeo ha perseguito l’obiettivo di creare un sistema sostanzialmente uniforme e, a questo scopo, ha individuato un’unica autorità di controllo (*Lead Authority*) identificata con riferimento al luogo dello stabilimento principale e/o unico del Titolare o del Responsabile, nel caso in cui questi ultimi effettuino trattamenti transfrontalieri. In questo modo, si eviterà che violazioni delle medesime norme del Nuovo Regolamento possano essere oggetto di ricorsi decisi diversamente a seconda dell’autorità di controllo di ciascun Paese. In ogni caso, il Regolamento, al fine di non escludere le altre autorità di controllo eventualmente coinvolte, introduce una serie di norme volte a garantire cooperazione e assistenza reciproca, tenendo conto che la decisione della *Lead Authority* sarà vincolante anche per i trattamenti effettuati dal Titolare in altri Stati e utilizzando dati di cittadini di altri Paesi dell’UE.

In conclusione, sicuramente il nuovo Regolamento pone obblighi di *compliance* particolarmente stringenti e rigorosi nei confronti degli operatori che trattano dati personali, tuttavia si ritiene opportuno rilevare che l’adozione di uno strumento normativo unico, con applicazione uniforme in tutta l’Unione Europea, dovrebbe agevolare sensibilmente l’esercizio del *business* delle aziende che non si troveranno più a fronteggiare l’incertezza giuridica scaturente dalla frammentazione delle normative di ciascun Paese e a sostenere i costi e la burocrazia conseguenti.

Avv. Simona Cardillo

Avv. Daniela Cardillo