diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

Protezione dei dati personali: come gestire il periodo transitorio ed impostare buone prassi

Autore: Redazione
In:

di Gloriamaria Paci e Luciano Delli Veneri

Dopo un iter durato oltre quattro anni, il 24 maggio 2016 è ufficialmente entrato in vigore il Regolamento 2016/679/UE sulla protezione dei dati personali (nel seguito anche "Regolamento") che dispiegherà la propria completa efficacia a partire dal prossimo 25 maggio 2018 quando dovrà essere garantito il perfetto allineamento fra la normativa nazionale in materia di protezione dati e le disposizioni del Regolamento.
Resta quindi un anno per prepararsi a questa importante scadenza. Un periodo di tempo che andrà utilizzato al meglio considerando i significativi cambiamenti che la norma ha introdotto.

Perché un Regolamento
Esaminiamo nel dettaglio il Regolamento per coglierne gli aspetti principali e valutarne i più significativi impatti. Prima di tutto è importante sottolineare che la scelta del Legislatore dello strumento del "Regolamento" ha voluto porre le basi affinchè a livello comunitario si creassero le condizioni per l'applicazione di una normativa unica in tutti i paesi superando quella che di fatto era una frammentazione che vedeva 28 differenti modi di concepire la protezione dei dati personali ed applicare la Direttiva 95/46/UE: infatti la direttiva privacy con le sue 28 diverse trasposizioni nel paesi Membri UE ha comportato e continua a comportare un quadro normativo frammentario e disomogeneo, che ha creato e crea squilibri, condizioni di sbilanciamento e diversità di regole per le organizzazioni (aziende, enti,...) che fanno business nella UE, incluso anche le organizzazioni extra UE.
Il Regolamento pone quindi le basi affinché, ad esempio, un Titolare italiano con sede/stabilimenti produttivi, sedi secondarie, filiali in altri Stati europei potrà fare affidamento sul fatto che la normativa sulla protezione di dati personali sarà, se non del tutto identica, almeno analoga a quella applicata in Italia: nella realtà almeno in una prima fase vi potranno essere delle differenze dovute alla esigenza di rendere omogenei contesti normativi ed applicativi che sono, in molti casi, significativamente differenti.
A titolo esemplificativo, in alcuni Stati le Autorità di controllo in materia di protezione dei dati personali non hanno poteri sanzionatori, in altri tutti i trattamenti devono essere notificati, in altri ancora non è previsto il consenso per l'impiego dei cookies. Ciò potrà interessare anche il nostro paese poiché, anche se il Regolamento è direttamente vincolante ed applicabile, vi è l'esigenza che il legislatore nazionale, d'intesa con il Garante italiano, intervenga per raccordare tutti i provvedimenti nazionali e renderli

Diritto & Diritti ISSN 1127-8579

coerenti con il nuovo quadro normativo europeo. Ciò che è estremamente importante, tutti i Titolari che raccolgono i dati personali dei propri Clienti, Dipendenti, etc. avranno gli stessi diritti e doveri e questo costituirà sicuramente una notevole semplificazione e, conseguentemente, una auspicata riduzione degli adempimenti e dei connessi costi.
Tale semplificazione riguarderà anche le Autorità di protezione dei dati personali (nel seguito anche DPA) poiché anche per costoro varrà il principio dei semplificazione che, di massima, consentirà al Titolare di avere a riferimento la DPA del proprio Stato nazionale e sarà questa poi a farsi carico della relazione con le altre DPA eventualmente chiamate in causa.

A chi si applica

Un altro aspetto estremamente importante riguarda l'ambito territoriale di applicabilità del regolamento indicato dall'art. 3 del regolamento che al c. 2 prevede che:
"Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione;
Si tratta sicuramente di uno dei punti cardini del Regolamento con il quale si è voluto perseguire un obiettivo di ribilanciamento della libera concorrenza tra imprese ponendo le basi per il superamento del vantaggio competitivo basato su di una più ampia libertà di azione che ha visto come sicure favorite molte multinazionali d'oltre oceano. In estrema sintesi, quindi, tutti i soggetti economici che intendono offrire servizi, anche non a pagamento, a "Interessati" che si trovano all'interno dei confini dell'Unione Europea devono rispettare le prescrizioni del Regolamento indipendentemente da dove ha sede l'azienda o dove si trovano gli apparati con i quali i trattamenti vengono effettuati.

Il Regolamento europeo 2016/679/UE ed i nuovi principi: Accountability – Privacy by design e by default

Accountability

Altra significativa innovazione introdotta dal Regolamento, sarebbe forse più giusto parlare di "cambio di paradigma", è il principio di "accountability", in italiano "Responsabilizzazione", introdotto dall'art. 5 c. 2 che recita: "Il titolare del trattamento è competente per il rispetto del paragrafo 1 [in ordine alla protezione dei dati personali- ndr] e in grado di comprovarlo («responsabilizzazione»)". Sul punto per meglio comprendere la portata di tale cambiamento di scenario è utile la lettura dei Considerando dal 74 al 79 che contribuiscono a chiarire come sia importante intendere che non avremo più come parametro di riferimento le c.d. "misure minime" del vecchio DPS, applicate le quali il Titolare potrà considerarsi "al sicuro da possibili contestazioni" ma si tratterà di una attività di valutazione che è rimessa alla sua

Diritto & Diritti ISSN 1127-8579

responsabilità: in estrema sintesi sarà il Titolare, o in sua vece il Responsabile del trattamento, che dovrà individuare ed applicare le misure idonee a garantire che il trattamento avvenga nel rispetto dei dettami normativi e senza rischi per le libertà e i diritti dell'Interessato. L'art. 24 del regolamento costituisce il principale riferimento al quale il Titolare dovrà prestare la massima attenzione al fine di dare concreta attuazione al principio di accountability e che, in estrema sintesi, traccia il quadro di riferimento al quale attenersi e che richiede, tra l'altro, che "Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario".

Privacy by design e by default

Sempre in ottica accountability il Titolare deve applicare il principio di "privacy by design", art. 25, che costituisce uno strumento indispensabile a creare le condizioni affinché alla protezione dei dati personali venga prestata la necessaria attenzione sin dalle fasi iniziali di progettazione di un prodotto/servizio/applicativo destinato a trattare dati personali. Una tale scelta consentirà di applicare fin da subito soluzioni e misure di protezione in grado di garantire adeguati livelli di tutela ai dati trattati adottando, ad esempio, forme di offuscamento di una parte di dati, pseudoanonimizzazione, o altre idonee misure di protezione. Sempre al fine di creare le condizione di minimizzazione dei rischi l'applicazione di modelli di "privacy by default" farà in modo che la raccolta, l'utilizzo, ma anche la conservazione dei dati personali sarà impostata nel rispetto del principio di necessità evitando, quindi, di raccogliere dati personali che non hanno utilità rispetto alle finalità perseguite e che costituirebbero solo un inutile aggravamento dei rischi e soprattutto di conservarli anche quando non ve ne sarebbe la necessità. Più in generale al Titolare è richiesto di garantire la "Sicurezza del trattamento", Art. 32, prestando le necessarie attenzioni alle misure tecniche ed organizzative che avendo a riferimento la tipologia dei trattamenti, le finalità perseguite, la probabilità di accadimento e di gravità dei rischi connessi per i diritti e le libertà degli individui, garantiscano un contesto protetto nel quale tali trattamenti vengono effettuati.

Violazione o Data breach

Una novità estremamente importante è l'introduzione dell'obbligo di notifica delle "violazioni" (data breach) che l'art. 33 del Regolamento estende a tutti i Titolari: in estrema sintesi ogni volta che si verifica una violazione di dati personali il Titolare deve notificare alla DPA competente l'accadimento entro 72 ore dal momento nel quale l'evento si è verificato o è stato rilevato. L'art. 4 c.12 definisce la "violazione dei dati personali" come "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati": quindi qualunque evento che comprometta la sicurezza o la confidenzialità dei dati personali nella disponibilità del Titolare dovrà essere notificata alla DPA con una descrizione dell'evento, delle categorie dei dati interessati, della numerosità dei soggetti coinvolti, dei

Diritto & Diritti ISSN 1127-8579

possibili rischi connessi nonché delle misure adottate o che si intende adottare per per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. Nel caso in cui la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all interessato senza ingiustificato ritardo: questo prescrive l art. 34 che però prevede eccezioni all obbligo di notifica all Interessato nel caso in cui ai dati personali siano state applicate misure di sicurezza che li abbiano resi incomprensibili a chiunque non sia autorizzato ad accedervi. Inoltre il Titolare è tenuto a documentare ogni violazione dei dati personali, le circostanze in cui si è verificata, le conseguenze nonché la descrizione delle attività svolte per porre rimedio o per limitare gli impatti dell evento: tale documentazione deve essere messa a disposizione della DPA in caso di controlli. Si tratta di un adempimento, già previsto e applicato in alcuni settori dalla normativa italiana (Telecomunicazioni, Banche, Sanità) o per il trattamento di particolari tipologie dei dati personali (dati biometrici) che richiede un notevole dispiego di energia poiché si dovranno implementare una serie di controlli sui processi di trattamento dei dati personali al fine di evitare le violazioni o, comunque, rilevarle tempestivamente per poter dar seguito alle previste attività di notifica.

Per approfondire l argomento:
Formazione
L applicazione della normativa sulla privacy negli Enti Pubblici: dal Decreto Legislativo n. 196/2003 al Regolamento UE 2016/679
Bologna, 30 maggio 2017
http://www.formazione.maggioli.it/corso/3831/l-applicazione-della-normativa-sulla-privacy-negli-enti-pubblici/
Roma, 8 giugno 2017
http://www.formazione.maggioli.it/convegno/1660/il-regolamento-generale-sulla-protezione-dei-dati-personali-quali-adempimenti-per-la-pubblica-amministrazione/

La nuova privacy
Nadia Arnaboldi, 2016, Maggioli Editore
Dopo oltre quattro anni di negoziati tra Commissione Eu- ropea, Parlamento e Consiglio, in data 4 maggio 2016 si è giunti alla pubblicazione del Regolamento europeo 2016/679 del 27 aprile 2016 “relativo alla protezione delle persone fisiche con...

39,00 € 35,10 € Acquista

Diritto & Diritti ISSN 1127-8579

su www.maggiolieditore.it

https://www.diritto.it/protezione-dei-dati-personali-come-gestire-il-periodo-transitorio-ed-impostare-buone-prassi/

Diritto & Diritti ISSN 1127-8579