26 giugno 2016 18:03

ITALIA: Diritto oblio e portabilita' dati online. Manuale Garante Privacy

Il diritto all'oblio e quello alla portabilità dei dati, la nuova figura del Responsabile della protezione dei dati, l'obbligo di comunicare le violazioni e gli attacchi informatici subiti, garanzie per il trasferimento dei dati fuori dall'Ue: sono alcuni degli aspetti del nuovo Regolamento europeo sulla protezione dei dati personali, entrato in vigore lo scorso 24 maggio e che sarà applicabile in tutti gli Stati dell'Unione a partire dal 25 maggio 2018, e che sono sintetizzati in un opuscolo on line messo a punto dal Garante, che inaugura una serie di iniziative informative per spiegarne la portata. Il Regolamento, spiega la guida consultabile sul sito del Garante, "introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento e per i casi di violazione dei dati".
Per fornire informazioni più chiare e complete "l'informativa diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti. Per facilitare la comprensione dei contenuti, si potrà fare ricorso anche a icone, identiche in tutta l'Unione europea. Gli interessati - precisa il Garante - dovranno sapere se i loro dati sono trasmessi al di fuori dell'Ue e con quali garanzie; cosi come dovranno sapere che hanno il diritto di revocare il consenso a determinati trattamenti, come quelli a fini di marketing diretto".
Il consenso al trattamento dei dati personali dovrà essere, "preventivo e inequivocabile", anche quando espresso attraverso mezzi elettronici. Per trattare i dati sensibili, il Regolamento "prevede che il consenso deve essere anche 'esplicito'. Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate. Il consenso potrà essere revocato in ogni momento". I fornitori di servizi Internet e i social media, si legge nella guida, "dovranno richiedere il consenso ai genitori o a chi esercita la potestà genitoriale per trattare i dati personali dei minori di 16 anni".
Un altro aspetto trattato riguarda le decisioni che producono effetti giuridici che "non potranno essere basate esclusivamente sul trattamento automatizzato dei dati". Faranno eccezione "i casi in cui l'interessato abbia rilasciato un consenso esplicito al trattamento automatizzato dei suoi dati", oppure se questo tipo di trattamento "risulti strettamente necessario per la definizione di un contratto o avvenga in base a specifici obblighi di legge". In ogni caso, sono previste garanzie per gli interessati, "come il diritto di opporsi alla decisione adottata sulla base di un trattamento automatizzato o il diritto di ottenere anche l'intervento umano rispetto alla decisione stessa".
Grazie all'introduzione del cosiddetto 'diritto all'oblio', si potrà ottenere la cancellazione dei propri dati personali anche on line da parte del titolare del trattamento se ricorrono alcune condizioni: se i dati sono trattati solo sulla base del consenso; se non sono più necessari per gli scopi rispetto ai quali sono stati raccolti; se sono trattati illecitamente; oppure se l'interessato si oppone legittimamente al loro trattamento. A questo diritto si accompagna l'obbligo di comunicare la richiesta di cancellazione a chiunque stia trattando i dati, nei limiti di quanto tecnicamente possibile. Il diritto all'oblio potrà essere limitato solo in alcuni casi: garantire l'esercizio della libertà di espressione o il diritto alla difesa in sede giudiziaria; tutelare un interesse generale; quando i dati, resi anonimi, sono necessari per la ricerca storica o per finalità statistiche o scientifiche.
Per garantire la libertà di trasferire i dati in un mercato digitale più aperto alla concorrenza, il Regolamento introduce il diritto alla 'portabilità' dei dati personali che potranno essere trasferiti da un titolare del trattamento a un altro. Ad esempio, si potrà cambiare il provider di posta elettronica senza perdere i contatti e i messaggi salvati.
Resta vietato il trasferimento di dati personali verso Paesi situati al di fuori dell'Unione europea o organizzazioni internazionali che non rispondono agli standard di adeguatezza in materia di tutela dei dati, rispetto ai quali il Regolamento introduce criteri di valutazione più stringenti.
E' introdotto anche l'obbligo di comunicare i casi di violazione dei dati personali (data breach). Il titolare del trattamento dovrà darne comunicazione all'Autorità nazionale di protezione dei dati. Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.
Imprese ed enti avranno più responsabilità, ma potranno beneficiare di semplificazioni. In caso di inosservanza delle regole sono previste sanzioni, anche elevate. Il Regolamento è direttamente applicabile e vincolante in tutti gli Stati membri dell'Unione europea e non richiede una legge di recepimento nazionale. Inoltre, si applica integralmente alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti a persone che si trovano nel territorio dell'Ue.
Il regolamento introduce un approccio basato sulla valutazione del rischio che premia i soggetti più responsabili. Il principio-chiave è 'privacy by design', ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problemi. Viene inoltre introdotta la figura del Responsabile della protezione dei dati (Data Protection Officer o

DPO), incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti. Sono poi previste semplificazioni per i soggetti che offrono maggiori garanzie e promuovono sistemi di autoregolamentazione. Il Regolamento introduce il ricorso a codici di condotta da parte di associazioni di categoria e altri soggetti, sottoposti all'approvazione dell'Autorità nazionale di protezione dei dati ed eventualmente della Commissione europea.
La certificazione potrà essere rilasciata da un soggetto abilitato oppure dall'Autorità di protezione dei dati.
L'adesione ai codici di condotta e la certificazione del trattamento saranno elementi di cui l'Autorità dovrà tenere conto, per esempio, nell'applicare eventuali sanzioni o nell'analizzare la correttezza di una valutazione di impatto effettuata dal titolare. Il Regolamento punta dunque a rispondere alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali sempre più avvertite dai cittadini dei Paesi dell'Unione europea.