Data Protection & GDPR
Misure di sicurezza informatiche ed assicurative nel trattamento dei dati personali

L'attuazione del GDPR in Italia: sfide e opportunità

Roma, Centro Congressi Confcommercio
(Sala Orlando)
martedì 25 ottobre 2016

Luigi Montuori

Lo stato del dossier ad oggi

- Regolamento generale (GDPR): approvazione Parlamento europeo 27 aprile 2016 n. 679/2016; pubblicazione in GUUE 4 maggio 2016

- Direttiva polizia e giustizia: approvazione Parlamento europeo 27 aprile 2016 n. 680/2016; pubblicazione in GUUE 4 maggio 2016

Il quadro internazionale: Promemoria

- Sentenze CGUE (Google Spain + Conservazione dati traffico + Weltimmo + Bara/Romania, Facebook/Schrems)
- Sentenze CEDU (libertà espressione/privacy)
- WP29 : pareri, raccomandazioni, contributi
- Consiglio d'Europa (Revisione Convenzione 108/81)
- Conferenza internazionale autorità PD

Il pacchetto in pillole

- Abrogazione Direttiva 95/46 + Abrogazione Decisione-quadro 2008/977
- Esecutività (Regolamento) / Trasposizione nazionale (Direttiva): 2 anni da entrata in vigore (25 maggio 2018)
- E nel frattempo?

Un unico Regolamento per tutti gli Stati

- Il Regolamento, a differenza di una direttiva, non richiede una legge di recepimento nazionale ed è direttamente applicabile e vincolante in tutti gli Stati dell'Unione europea.
- Il Regolamento si applica integralmente alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione europea. Quindi, tutte le aziende dovranno rispettare le stesse regole, sia dentro sia fuori dall'UE.

Le novità in sintesi

- **Regolamento:**
- Diritti interessati: trattamenti ulteriori, portabilità, «oblio»
- Obblighi titolari: approccio basato sul rischio (privacy by design, DPO, valutazione di impatto, notifica data breach, certificazione…) + «Accountability»
- Ruolo Autorità: Sportello unico e meccanismo di coerenza, il Board, Sistema sanzionatorio
- **Direttiva polizia e giustizia:**
- trattamenti e trasferimenti di dati

Informativa più chiara e completa sul trattamento

- Chi tratta dati personali deve fornire informazioni più ampie alle persone interessate dal trattamento (per esempio, se i dati sono trasmessi all'estero e con quali garanzie; il diritto di opporsi a determinati trattamenti, per esempio quelli per finalità di marketing diretto), anche se raccoglie i dati da altre fonti.
- Per facilitare l'informazione degli interessati, i titolari potranno utilizzare delle icone che sintetizzano i contenuti dell'informativa. Le icone saranno identiche in tutta l'Unione europea

Regole più chiare per il consenso

- Il consenso della persona interessata dovrà essere "inequivocabile" e, come oggi, dovrà precedere il trattamento ed "esplicito" per trattare dati sensibili.
- Il Regolamento vieta ogni forma di consenso tacito o implicito e prevede che non può essere raccolto proponendo a un interessato una serie di opzioni già selezionate.
- per i fornitori di servizi via Internet sono previste condizioni più stringenti per il consenso dei minori di 16 anni, con intervento obbligatorio dei genitori o di chi detiene la potestà genitoriale.

Decisioni che producono effetti giuridici su una persona e si basano esclusivamente su trattamenti automatizzati

- Sono vietate le decisioni che si basano esclusivamente su trattamenti automatizzati (come la profilazione) e producono effetti giuridici su una persona (ad esempio, la concessione di un prestito o di uno sconto), a meno che la persona interessata abbia dato il consenso esplicito a questi trattamenti o i trattamenti siano necessari in base a un contratto o a obblighi specifici di legge. (Art. 22(1), (2)
- Disposizione non diversa da quella dell'art. 14.1 del nostro Codice, derivante a sua volta da art. 15 direttiva 95/46

Sono comunque previste garanzie per gli interessati:

- diritto di opporsi alla decisione presa sulla base di un trattamento automatizzato effettuato con il consenso o per contratto;
- diritto di ottenere l'intervento umano in questi stessi casi. (Art. 22.3)

Diritto all'opposizione - Regolamento

- In generale, l'interessato ha il diritto di opporsi a qualunque trattamento (compresa la profilazione), in modo motivato, salvo che il titolare dimostri l'interesse legittimo oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. (Art. 21.1)
- L'interessato ha il diritto di opporsi alla profilazione senza dover motivare la propria opposizione. (Art. 21.2) quando il trattamento di profilazione è in qualche modo collegato ad attività di marketing diretto

Diritto all'oblio e diritto alla portabilità dei dati

- L'interessato ha il diritto non solo di ottenere la cancellazione dei propri dati personali, se questi sono trattati dal titolare solo sulla base del consenso ovvero non sono più necessari per il trattamento, oppure se vengono trattati illecitamente o la persona si è opposta al loro trattamento secondo quanto prevede il Regolamento, ma anche di ottenere che il titolare informi di questo obbligo chiunque abbia avuto da lui quei dati (comprese copie o link): è il cosiddetto "diritto all'oblio".
- Il diritto all'oblio può essere limitato per tenere conto di altre esigenze e interessi legittimi: per esempio, la libertà di espressione, un interesse pubblico, o le esigenze dell'attività archivistica.

- Oltre alla cancellazione, si potrà chiedere la "limitazione" del trattamento, cioè di "congelare" un dato in attesa di stabilire se non sia realmente più necessario per le finalità di quel trattamento oppure per utilizzarlo anche successivamente, in particolare in un procedimento giudiziario che coinvolga la persona interessata.
- Ogni interessato avrà diritto alla portabilità dei propri dati (quelli da lui forniti al titolare sulla base del consenso o per obblighi contrattuali), compreso il diritto di ottenere che il titolare trasferisca quei dati a un altro titolare a scelta dell'interessato. Vi sono delle eccezioni, in particolare per i dati contenuti in archivi di interesse pubblico.

Garanzie più rigorose per il trasferimento dei dati extra UE

- Resta vietato il trasferimento di dati personali verso Paesi extra-Ue o organismi internazionali che non garantiscono una tutela definita "adeguata" dalla Commissione europea.
- Vengono introdotti requisiti più stringenti per questa valutazione di adeguatezza, che dovrà essere condotta a 360 gradi sull'insieme delle norme e dei meccanismi effettivi di tutela nel Paese di destinazione.
- i titolari potranno continuare ad utilizzare per il trasferimento specifiche garanzie contrattuali se manca una decisione di adeguatezza della Commissione. Il Regolamento introduce norme dettagliate e vincolanti sulle caratteristiche e i contenuti di questi strumenti contrattuali (clausole contrattuali modello, norme vincolanti di impresa - BCR).

- Come ulteriore e più limitata deroga, si potrà ricorrere, ad esempio, al consenso dell'interessato o invocare specifici obblighi contrattuali da parte dell'interessato oppure un interesse pubblico importante dello Stato membro.
- Il Regolamento vieta anche di trasferire dati richiesti da autorità giudiziarie o amministrative di Paesi terzi se il trasferimento non è effettuato sulla base di accordi internazionali di mutua assistenza giudiziaria o attraverso strumenti analoghi.

Diritto di notifica in caso di grave compromissione dei dati

- Ogni persona i cui dati personali siano violati ha il diritto di esserne informata dal titolare e di ricevere indicazioni su come il titolare intende limitare le possibili conseguenze negative.
- Il titolare può decidere di non informare gli interessati se ritiene che la violazione non comporti un rischio elevato per i loro diritti (ad esempio, frode, furto di identità, danno di immagine, ecc.), oppure se dimostra di avere adottato misure di sicurezza (come la cifratura) a tutela dei dati violati ovvero che fornire l'informazione alle persone interessate comporterebbe uno sforzo sproporzionato.
- Se il titolare dimostra che informare gli interessati della violazione comporterebbe uno sforzo sproporzionato, gli interessati hanno comunque il diritto di esserne messi a conoscenza in altro modo (ad esempio, tramite un'inserzione su un quotidiano o una notifica sul sito web del titolare).
- L'Autorità può imporre a un titolare di informare gli interessati sulla base di una propria valutazione del rischio associato alla violazione.

Lo sportello unico (OSS)

- le imprese stabilite in più Stati membri o che offrono prodotti e servizi da un Paese dell'Unione europea rivolgendosi a clienti e utenti in altri Paesi dell'Ue avranno un solo interlocutore per quanto riguarda il rispetto del Regolamento, ossia l'Autorità garante del Paese dove si trova il loro stabilimento principale o unico. Questo semplificherà la gestione dei trattamenti e garantirà un approccio uniforme.

Responsabilizzazione/accountability

- Il Regolamento promuove l'adozione di approcci e politiche che tengano conto del rischio che un trattamento di dati personali può comportare
- assicurare la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema "*privacy by design*".
- Comportamenti che consentano di prevenire possibili problematiche: ad esempio, l'obbligo per i titolari/responsabili di condurre una valutazione di impatto prima di procedere ad un (nuovo) trattamento, sentendo l'Autorità garante in caso di dubbi, o di nominare in alcuni casi un "Responsabile della protezione dati" (ovvero il "Data Protection Officer") per assicurare una gestione corretta e proattiva dei dati personali trattati.
- Sono eliminati alcuni oneri considerati puramente burocratici quali la notifica dei trattamenti all'Autorità garante, o l'obbligo di ottenere l'autorizzazione dell'Autorità garante per i trattamenti considerati "a rischio" (purché sia condotta la valutazione di impatto e si consulti l'Autorità in caso di dubbi).

- Il Regolamento promuove il ricorso a codici deontologici da parte di associazioni di categoria e altri soggetti, sottoposti all'approvazione delle DPA ed eventualmente della Commissione (in tal caso, il codice deontologico avrà applicazione nell'intera UE).
- Il Regolamento introduce la possibilità per il titolare di far certificare i propri trattamenti, in misura parziale o totale, anche ai fini di trasferimenti di dati in Paesi terzi; la certificazione può essere rilasciata da un soggetto a ciò abilitato ovvero dall'Autorità garante.
- I Garanti dovranno tenere conto dell'adesione a codici deontologici e/o schemi di certificazione nel valutare eventuali violazioni del Regolamento da parte di un titolare e, più in generale, nell'analizzare i risultati della valutazione di impatto condotta da un titolare.