Il Regolamento europeo sulla protezione dei dati personali
Le principali novità

17° Meeting nazionale ACEF 2017
Bologna, 9 novembre 2017

Claudia Cevenini

Professore a contratto di Diritto dell'informatica – Scuola di Ingegneria Università di Bologna
Dottore commercialista – Revisore legale

Panoramica

- Pubblicato nella GUCE L119 del 4 maggio 2016
- Entrato in vigore il 24 maggio 2016
- Si applica a decorrere dal **25 maggio 2018**
- Abroga la direttiva 95/46/CE dalla stessa data
- **Direttamente applicabile** in tutti gli stati membri
- **Margine di autonomia agli stati membri** su alcuni ambiti

Ambito di applicazione territoriale

Il Regolamento si applica al trattamento di dati personali:

A) effettuato da titolare o responsabile stabilito nell'UE, indipendentemente dal luogo di trattamento dei dati

NOVITA'

B) effettuato da titolare o responsabile **non stabilito nell'UE**, se riguarda dati di **interessati che si trovano nell'UE**:

- per l'**offerta di beni o la prestazione di servizi** o
- per **monitorare il loro comportamento all'interno dell'UE**.

Informativa – cosa cambia 1

Ulteriori informazioni da inserire

- Dati di contatto del **Data Protection Officer** (se previsto)
- La **base giuridica del trattamento** (es. consenso)
- Ove applicabile, l'intenzione del titolare di **trasferire dati personali a un paese terzo** e informazioni su ciò che rende il trasferimento legale (es. garanzie appropriate, ecc.)
- **Periodo di conservazione dei dati o**, se non è possibile, i **criteri** utilizzati per determinare tale periodo.
- Informazioni sull'eventuale **profilazione** degli interessati.
- **Diritto** di presentare un **reclamo** all'autorità di controllo.

Informativa – cosa cambia 2

Modalità dell'informativa

- Deve avere **forma concisa, trasparente, intelligibile** per l'interessato e **facilmente accessibile**.
- Occorre utilizzare un **linguaggio chiaro e semplice**.
- Per i **minori** occorre prevedere informative idonee.
- L'informativa è fornita, in linea di principio, **per iscritto**, anche se sono ammessi altri mezzi, quindi potrebbe essere data anche oralmente, ma nel rispetto del Regolamento.

Consenso – cosa cambia 1

Il consenso deve essere manifestato con una "**dichiarazione o azione positiva inequivocabile**".

Il consenso non deve essere necessariamente "documentato per iscritto", né è richiesta la "**forma scritta**", anche se questa è modalità **idonea** a configurare l'**inequivocabilità del consenso** e il suo essere "**esplicito**" (per i dati sensibili).

Il Titolare deve essere in grado di **dimostrare** che l'interessato ha prestato il proprio **consenso** a uno specifico trattamento.

Non devono essere predisposte caselle pre-spuntate sui moduli.

Consenso – cosa cambia 2

Se il consenso è prestato nel contesto di una **dichiarazione scritta che riguarda anche altre questioni**, la richiesta di consenso è:

- presentata in modo **chiaramente distinguibile** dalle altre materie,
- in forma **comprensibile** e **facilmente accessibile**,
- con un **linguaggio semplice e chiaro**.

Nessuna parte di una tale dichiarazione che violi il regolamento è vincolante.

Se l'esecuzione di un contratto è **condizionata** al **consenso non necessario**, questo potrebbe considerarsi **non liberamente prestato**.

Cosa succede ai consensi già ottenuti?

Il consenso ottenuto prima del 25 maggio 2018 resta valido se ha tutte le caratteristiche del Regolamento.

In caso contrario, occorre **raccogliere nuovamente il consenso degli interessati conformemente alle nuove regole**.

In particolare, occorre verificare che la richiesta di consenso sia **chiaramente distinguibile** da altre richieste o dichiarazioni fornite all'interessato (es. altri moduli, informativa per determinati interventi, ecc.).

I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali.

Figure del trattamento - incaricati

Il **Regolamento non prevede espressamente** la figura dell'**incaricato** del trattamento ma **non la esclude**.

Il Regolamento fa riferimento a **persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile**.

Queste figure possono essere ad es. i collaboratori di studio.

Figure del trattamento – cosa cambia 1

Designazione dei responsabili del trattamento

Deve avvenire con un **contratto** (o altro **atto giuridico conforme al diritto nazionale**).

Oltre a specificare i compiti, l'atto ha un **contenuto tassativo**, deve indicare ad es.:

- la natura, durata e finalità del trattamento o dei trattamenti assegnati,
- le categorie di dati oggetto di trattamento,
- le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e del regolamento, ecc.

Il responsabile deve fornire **garanzie sufficienti** (es. mediante adesione a codici deontologici).

Figure del trattamento – cosa cambia 2

La figura del sub-responsabile

I **responsabili** possono a loro volta **nominare dei sub-responsabili** del trattamento, per **specifiche attività d**i trattamento, con l'autorizzazione scritta del Titolare.

I sub-responsabili devono rispettare gli **stessi obblighi contrattuali** a cui è soggetto il responsabile primario nei confronti del titolare.

Il responsabile primario risponde nei confronti del titolare dell'inadempimento dell'eventuale sub-responsabile, a meno che non dimostri che l'evento dannoso non può essergli in alcun modo imputabile.

Figure del trattamento – cosa cambia 3

Obblighi dei responsabili

I responsabili hanno obblighi specifici, distinti da quelli dei rispettivi titolari.

- Tenuta del **registro** dei trattamenti svolti.
- Adozione di idonee misure tecniche e organizzative per garantire la **sicurezza** dei trattamenti.
- Designazione di un data protection officer (**responsabile della protezione dei dati**), nei casi previsti dal Regolamento o dal diritto nazionale.

Responsabilizzazione

I titolari e i responsabili devono essere in grado di **dimostrare** di avere concretamente adempiuto agli obblighi del Regolamento.

Deve essere effettuata una **valutazione di impatto**, per determinare i possibili rischi del trattamento e le misure tecniche e organizzative da adottare per mitigare possibili rischi.

Notifica al Garante

NON è più prevista la notificazione preventiva al Garante.

Se i titolari evidenziano rischi particolari dopo avere effettuato la valutazione di impatto, possono consultare il Garante per avere indicazioni su come gestire tali rischi.

Registro dei trattamenti

I titolari e i responsabili del trattamento devono tenere un **registro delle attività di trattamento** qualora:

1) effettuino **trattamenti a rischio** per i diritti e le libertà dell'interessato, il **trattamento non** sia **occasionale o includa** il trattamento di **categorie particolari di dati** (= **dati relativi alla salute**) o

2) abbiano **più di 250 dipendenti**.

Il Garante invita tutti i titolari e i responsabili, a prescindere dalle dimensioni, a predisporre tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche.

Misure di sicurezza

Devono garantire un **livello di sicurezza adeguato al rischio** del trattamento.

NON vi saranno più obblighi generalizzati di adozione di **misure "minime" di sicurezza**.

La valutazione dovrà essere effettuata dal titolare e dal responsabile, caso per caso, tenendo conto dei rischi specificamente individuati, es. distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Violazioni di dati personali

I titolari dovranno **notificare** al **Garante** le **violazioni di dati personali** di cui vengano a conoscenza, entro 72 ore **se** ritengono **probabile** che possano esservi **rischi** per i diritti e le libertà degli interessati. La notifica non è obbligatoria, ma è subordinata alla valutazione del rischio per gli interessati da parte del titolare.

Se la **probabilità** di questo **rischio** è **elevata**, dovranno essere **informati** della violazione anche gli **interessati**.

I titolari dovranno **documentare** le **violazioni** di dati personali subite - anche se non notificate al Garante e non comunicate agli interessati - nonché le relative **circostanze** e **conseguenze** e i **provvedimenti** adottati.

Responsabile della protezione dei dati

In alcuni casi è obbligatorio designare un **responsabile della protezione dei dati** (**RPD**, o DPO: Data Protection Officer), es.:

a) trattamento effettuato da un'**autorità pubblica** o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala**; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel **trattamento, su larga scala**, di **categorie particolari di dati** personali.

Link utili

Garante privacy – pagina informativa sul Regolamento
http://www.garanteprivacy.it/web/guest/regolamentoue

Il testo integrale del Regolamento
http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT

La Guida del Garante privacy
http://194.242.234.211/documents/10160/5184810/Guida+al+nuovo+Regolamento+europeo+in+materia+di+protezione+dati

Grazie per l’attenzione!