Il nuovo Regolamento europeo sulla privacy

European Commission

Avv. Prof. Stefano Aterno

Il nuovo Pacchetto protezione dati

- Il “Pacchetto protezione dati” è stato **pubblicato** sulla Gazzetta Ufficiale dell’Unione Europea (GUUE) il 4 maggio 2016.
- ha l’obiettivo di garantire una **disciplina** sulla protezione dei dati personali **uniforme ed omogenea in tutta la UE.**

- Il Regolamento è **entrato in vigore il 25 Maggio 2016**; i Paesi dell’Unione Europea, in questo periodo hanno avuto il tempo **per porre in essere gli adeguamenti** richiesti dalla normativa in questione alle proprie politiche per la protezione ed il trattamento dei dati personali.

- **Dal 25 maggio 2018 il Regolamento sarà definitivamente applicabile in via diretta in tutti i Paesi UE**, considerato che non vi è la necessità di recepimento con atti nazionali (anche se non poche disposizioni lasciano liberi gli Stati Membri - o richiedono agli stessi - di introdurre ulteriori regole e condizioni).

I principali obiettivi della riforma

- Aggiornare la normativa “secondaria” alla luce dei Trattati di Lisbona

- Maggiore armonizzazione nell’Unione
- (dalla frammentazione a “una sola voce” specie su ciò che ha una dimensione internazionale)

- Un “tagliando” a norme superate, per essere al passo con le nuove tecnologie

Struttura degli argomenti trattati dal GDPR

- **Considerando**: Art da 1 a 173
- CAPO 1 **Disposizioni Generali**: art da 1 a 4
- CAPO 2 **Principi**: art da 5 a 11
- CAPO 3 **Diritti dell'Interessato**:
  - Sezione 1 Trasparenza e modalità: art 12
  - Sezione 2 Informazione e accesso i dati personali: art da 13 a15
  - Sezione 3 Rettifica e cancellazione: art da 16 a 20
  - Sezione 4 Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche: art da 21 a 22
  - Sezioni 5 Limitazioni: art 23
- CAPO 4 **Titolare del trattamento e responsabile del trattamento**:
  - Sezione 1 Obblighi generali: art da 24 a 31
  - Sezione 2 Sicurezza dei dati personali: art 32 a 34
  - Sezione 3 Valutazione di impatto sulla protezione dei dati personali e consultazione preventiva: da art 35 a 36
  - Sezione 4 Responsabile della protezione dei dati: da art 37 a 39
  - Sezione 5 Codice condotta e certificazione: art da 40 a 43
- CAPO V **Trasferimento di dati personali verso paesi terzi o organizzazioni internazionali**: art da 44 a 50
- CAPO VI **Autorità di Controllo indipendenti**:
  - Sezione 1 Indipendenza: art da 51 a 54
  - Sezione 2 Competenza, compiti e poteri: art da 55 a 59
- CAPO VII **Cooperazione e coerenza**:
  - Sezione 1 Cooperazione: art da 60 a 62
  - Sezione 2 Coerenza: art da 63 a 67
  - Sezione 3 Comitato europeo per la protezione dei dati: art da 68 a 76
- CAPO VIII **Mezzi di ricorso, responsabilità e sanzioni**: art da 77 a 84
- CAPO IX **Disposizioni relative a specifiche situazioni di trattamento**: art da 85 a 99

Articolo 7

Condizioni per il consenso (C42, C43)

Articolo 8

Condizioni consenso minori (rispetto ai social media)

Articolo 9

Trattamento di categorie particolari di dati personali (non solo dati relativi alla salute)

Articolo 12

Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato (C58-C60, C64)

Articolo 28

Responsabile del trattamento (C81)

Sintesi delle principali novità del Regolamento

- **Principio di responsabilizzazione** (cd. principio di accountability)
- **Privacy by design e by default**
- **Sicurezza del trattamento**: parametri per la valutazione dei costi di attuazione in rapporto al rischio
- **Data breach**: notifica tempestiva sulle violazioni dei dati personali
- **Registro delle attività di trattamento**
- **PIA (Privacy Impact Assessment)**
- **DPO (Data Protection Officer)**
- **Diritto all'oblio**
- **Data portability**

Principio di responsabilizzazione (cd. principio di accountability) (art. 5, co. 2)

Il Titolare del trattamento dovrà <u>comprovare</u> l'adozione di politiche privacy e di misure tecniche e organizzative adeguate per garantire (e quindi essere sempre anche in grado di dimostrare) la conformità al Regolamento

proattività

È l'applicazione operativa del principio di rendicontazione (o di "accountability"), secondo cui il Titolare del trattamento deve conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità, indicando obbligatoriamente - per ognuno di essi - una serie **nutrita** di informazioni, tali da assicurare e comprovare la conformità di ciascuna operazione alle disposizioni del Regolamento

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 25)

- Principio della «**Privacy by design**» dal quale discende l'attuazione di adeguate misure tecniche ed organizzative sia all'atto della progettazione che dell'esecuzione del trattamento

- Principio della «**Privacy by default**» che ricalca il **principio di necessità** di cui al vigente Codice privacy, stabilendo che i dati vengano trattati solamente per le finalità previste e per il periodo strettamente necessario a tali fini

prevedere meccanismi di protezione dei dati fin dalla progettazione delle attività e per l'intera gestione del ciclo di vita dei dati - dalla raccolta alla cancellazione - incentrandosi sistematicamente sulle garanzie procedurali in merito all'esattezza, alla riservatezza, all'integrità, alla sicurezza ed alla cancellazione dei dati.

Sicurezza del trattamento e misure di sicurezza (art. 32)

attuale normativa privacy

- quelle minime (predefinite ed indicate nell'Allegato B al Codice Privacy)
- quelle idonee (individuate a seguito di analisi del rischio e in relazione alle conoscenze acquisite, al progresso tecnologico, alla natura dei dati ed alle specifiche del trattamento);
- quelle prescritte dal Garante Privacy (mediante i Provvedimenti generali e specifici).

domani con il Regolamento

Il Titolare del trattamento deve mettere in atto **misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio**.

Continua: Sicurezza dei dati e del trattamento(art. 32)

In particolare tenendo conto:

dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche,

il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la **pseudonimizzazione** e la **cifratura** dei dati personali;
b) la capacità di assicurare su base permanente la **riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi** di trattamento;
c) la capacità di **ripristinare tempestivamente la disponibilità e l'accesso dei dati** personali in caso di incidente fisico o tecnico;
d) una **procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento**».

Valutazione d'impatto sulla protezione dei dati (cd. PIA) (art. 35)

quando un tipo di trattamento
può presentare un rischio elevato per i diritti e le libertà delle persone fisiche

il Titolare **prima di procedere al trattamento** dei dati deve effettuare una **valutazione dell'impatto** dei trattamenti ("**Privacy Impact Assessment**" cd. **PIA**)

SE la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento

si dovrebbe consultare l'autorità di controllo.

Il Titolare del trattamento nel svolgere la PIA si consulta con il Responsabile della protezione dei dati, se designato.

La PIA è richiesta in particolare nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche

b) il trattamento, su larga scala, di categorie particolari di dati personali (quali quelli concernenti la vita sessuale, lo stato di salute, la razza e l'origine etnica, dati genetici o dati biometrici) o di dati relativi a condanne penali e a reati;

c)la sorveglianza sistematica su larga scala di una zona accessibile al pubblico

La **PIA contiene** almeno:

- una **descrizione sistematica dei trattamenti** previsti e delle **finalità del trattamento**, compreso, ove applicabile, l'**interesse legittimo perseguito** dal Titolare del trattamento

- una **valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità**

- una **valutazione dei rischi per i diritti e le libertà degli interessati**

- le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone.

Certificazioni e codici condotta

L’adesione a codici di condotta o la presenza di certificazioni può essere elemento per dimostrare la conformità a requisiti di sicurezza sopra richiamati (art. 32 comma 3)

(non obbligatorietà)

Trattamento dati come «attività pericolosa»

- Risarcimento danni cagionato a chiunque (art. 82, 1)
- Il titolare, il responsabile, i contitolari (art. 82, 2,4 e 5
- Nesso causale e inversione dell'onere della prova
- Eventi dannosi non imputabili: caso fortuito e forza maggiore (art. 82, 3)
- Danni anche immateriali
- Responsabilità quasi oggettiva

Notifica di una violazione di dati personali all'autorità di controllo (cd. data breach) (art. 4.12; art. 33, 34)

Con la nozione di **violazione dei dati personali** (c.d. "personal data breaches"), si intende: la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso, in modo accidentale o illecito, ai dati personali trasmessi, conservati o comunque trattati.

Il **Titolare** del trattamento, in caso di una violazione come sopra descritta,

dovrà mettere in atto, **senza ingiustificato ritardo**, **due differenti azioni**:

notificazione della violazione

all'**Autorità di controllo**

segnalazione della violazione al **diretto interessato** (se rischio elevato per diritti e libertà delle persone fisiche)

Il **Responsabile** del trattamento **informa il Titolare** del trattamento **senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione**.

Registri delle attività di trattamento (art. 30)

Il **Registro delle attività di trattamento** ricalca, sotto alcuni profili, una parte del famoso Documento Programmatico per la Sicurezza (D.P.S.) previsto dal Codice della Privacy fino al 2012.

Ogni Titolare del trattamento tiene un registro delle attività di trattamento svolte sotto la propria responsabilità.

Il Registro del Titolare deve riportare:

- gli estremi del **Titolare** o del **Responsabile** del trattamento e, ove presente, del **Responsabile della protezione dei dati**
- le **finalità** del trattamento
- una descrizione delle categorie di **interessati** e di **dati** oggetto del trattamento e delle categorie di **destinatari cui i dati vengono comunicati**
- ove applicabile, i **trasferimenti di dati** personali verso un paese terzo o un'organizzazione internazionale
- ove possibile, i **termini ultimi previsti per la cancellazione** delle diverse categorie di dati
- ove possibile, una descrizione generale delle **misure di sicurezza tecniche e organizzative**

Valutazione d'impatto sulla protezione dei dati (cd. PIA) (art. 35)

È necessario effettuare una valutazione dell'impatto dei trattamenti ("Privacy Impact Assessment" cd. PIA) quando un tipo di trattamento:

-può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Il Titolare del trattamento nel svolgere la PIA si consulta con il Responsabile della protezione dei dati, se designato

La PIA è richiesta in particolare nei casi seguenti:

a) una **valutazione sistematica** e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la **profilazione,** e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche

b) il trattamento, **su larga scala, di categorie particolari di dati personali** (quali quelli concernenti la vita sessuale, salute, la razza e l'origine etnica, dati genetici o dati biometrici) o di dati relativi a condanne penali e a reati

c) **la sorveglianza sistematica** su larga scala di una zona accessibile al pubblico

La **PIA contiene** almeno:

- una **descrizione sistematica dei trattamenti** previsti e delle **finalità del trattamento**, compreso, ove applicabile, l'**interesse legittimo perseguito** dal Titolare del trattamento

- una **valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità**

- una **valutazione dei rischi per i diritti e le libertà degli interessati**

- le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone.

Designazione del Responsabile per la protezione dei dati (cd. Data Protection Officer “DPO”) (art. 37)

Il Titolare del trattamento e il Responsabile del trattamento designano sistematicamente un **Responsabile della protezione dei dati** ogniqualvolta:

- il trattamento è effettuato da **un'autorità pubblica o da un organismo pubblico**

- le attività principali del Titolare del trattamento 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**;

- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel **trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati**.

Il DPO va ad affiancarsi ai ruoli già presenti nel vigente Codice privacy di "Titolare", "Responsabile" e "Incaricato" del trattamento dei dati.

segue DPO

è **designato** in funzione delle **qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati**, e della **capacità** di assolvere i **compiti** di cui all'articolo 39 ovvero:

- è una designazione obbligatoria, ex lege, in alcuni casi (art. 37 comma 1);
- deve essere tempestivamente **coinvolto** in tutte le questioni relative alla protezione dei dati personali; (art. 38)
- **è sostenuto e supportato** dal Titolare e dal Responsabile per l'esecuzione dei suoi compiti e accessi; (art. 38)
- **non può ricevere alcuna** istruzione per l'esecuzione di tali compiti propri. **Non è rimosso o penalizzato** per aver adempiuto al suo dovere (art. 38);
- **riferisce direttamente** al vertice gerarchico del Titolare o del Responsabile del trattamento (art. 38 comma3);
- i terzi interessati possono contattare direttamente il DPO;
- **è tenuto al segreto e alla riservatezza;**
- può svolgere altri compiti e funzioni salvo la verifica di eventuali **conflitti di interesse.**

Articolo 38

Posizione del responsabile della protezione dei dati

1. *Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione* sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti.

   Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
4 Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
5 Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
6 Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Articolo 39

- ***Compiti del responsabile della protezione dei dati***

- ***1.Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:***
- ***a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;***
- ***b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;***
- ***c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; d) cooperare con l'autorità di controllo; e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. 2.Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.***

Riconoscimento di nuovi diritti

- **<u>Diritto alla cancellazione</u> dei dati (cd. “diritto all’oblio” ma non solo) (art. 17)**

  Ricorrendo determinate condizioni, per diritto all’oblio si intende la **possibilità per l'interessato di ottenere dal Titolare del trattamento la cancellazione dei dati personali** che lo riguardano senza ingiustificato ritardo

- Diritto alla portabilità dei dati (art. 20):

Ricorrendo determinate condizioni **l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico :**

- i dati personali che lo riguardano forniti a un Titolare del trattamento

e ha il diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti, qualora l'interessato abbia fornito il proprio consenso al trattamento o se questo sia necessario per l'esecuzione di un contratto

Responsabilità e responsabilizzazione conferma del criterio soggettivo ex art. 2050 cc

Il titolare e tutti coloro che sono coinvolti nel trattamento dei dati personali

(responsabile del trattamento -interno ed esterno- e incaricati)

sono obbligati

a fare tutto il possibile per evitare il danno

(eventuale, possibile, caso fortuito, forza maggiore)

e sono tenuti a dimostrarlo (rendicontazione)

Inversione onere della prova

Sanzioni amministrative pecuniarie (art. 83)

- Il Regolamento ha aumentato l'ammontare delle sanzioni amministrative pecuniarie, che potranno arrivare fino ad un massimo di 20 milioni di Euro o fino al 4% del fatturato mondiale totale annuo, lasciando peraltro ciascuno Stato membro libero di adottare norme relative ad altre sanzioni.

- Sanzioni equivalenti per le violazioni negli Stati membri. Tali sanzioni devono essere effettive, proporzionate e dissuasive.

- Gli Stati membri dovranno stabilire disposizioni ad hoc relative a **sanzioni penali** per le violazioni del presente regolamento

- La mancata previsione di minimi edittali consente di valutare, nella dosimetria della pena da infliggere, una pena anche nel minimo molto bassa nei **casi di lieve rilevanza**. Il vecchio codice prevedendo invece delle pene minime talvolta eccessivamente alte obbligava al pagamento di importi spropositati rispetto al fatto concreto.

Il futuro della privacy con il Regolamento

-<u>Il quadro normativo privacy è in via di definizione a breve termine</u>

- non poche disposizioni del Regolamento lasciano liberi gli **Stati membri** – o richiedono agli stessi – di introdurre **ulteriori regole e condizioni**

- il **Legislatore italiano** sta emanando un provvedimento normativo (legge delega) per individuare quali delle **norme del vigente Codice privacy saranno abrogate** e quali resteranno in vigore perché non in conflitto con il Regolamento (adeguamento)

- **sulla vigenza dei provvedimenti** dallo stesso finora emanati alla luce del Codice privacy probabilmente si deciderà caso per caso se potrà farsi riferimento ad essi e in che modo

Domande ?

resto a disposizione

per qualsiasi chiarimento

Avv. Prof. Stefano Aterno

s.aterno@studioaterno.it

European Commission