Marco Cuniberti
(Avvocato in Mondovì - Gruppo di Studio Privacy OPEN Dot Com)

Il nuovo regolamento europeo Privacy GDPR - Reg. n. 679/2016 UE

Responsabilizzazione del Titolare

Principio dell'accountability (o "responsabilizzazione") del Titolare, che deve **dimostrare la conformità delle attività di trattamento al Regolamento, compresa l'efficacia delle misure adottate**.

Art. 24

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 mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente alla legge.

Responsabilizzazione del Titolare

Il titolare deve conoscere i concetti e le regole fondamentali sul trattamento dei dati personali.

Il Regolamento impone che ogni titolare del trattamento faccia in modo che il trattamento sia lecito sotto ogni profilo, e, soprattutto, sia in grado di comprovarlo.
Deve riesaminare le politiche interne in tema di trattamento di dati personali, provvedendo anche a definire in maniera adeguata i ruoli e assicurarsi che tutti coloro che trattano dati personali ricevano adeguate istruzioni e formazione (ex art. 29 del GDPR)

Privacy by design (fin dalla progettazione)

Art. 25: Protezione dei dati fin dalla progettazione

Sia al momento di determinare i mezzi del trattamento (di progettare, disegnare il sistema), sia all'atto del trattamento stesso il titolare adotta misure tecniche e organizzative adeguate (quali la pseudonimizzazione) volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati

Privacy by design (fin dalla progettazione)

Art. 25

Ciò, tenendo conto:
dello stato dell'arte
dei costi di attuazione
della natura del trattamento
dell’ambito di applicazione del trattamento
del contesto e delle finalità del trattamento
dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento

Privacy by default (per impostazione predefinita)

Il titolare del trattamento attua misure tecniche e organizzative adeguate per garantire che siano trattati, **per impostazione predefinita (di default)**, **solo i dati personali necessari per ciascuna finalità** del trattamento (cioè quelli indispensabili, principio di “minimizzazione”)

Obbligo che vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità ai dati stessi.

Il titolare implementa sin dall’inizio (by design) un sistema in cui, tutte le operazioni concernenti trattamenti di dati personali di persone fisiche, siano di default privacy oriented.

Privacy by default (per impostazione predefinita)

Un consiglio

“Procedere alla verifica dei sistemi informatici, per assicurare il rispetto dei principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita di cui all’art. 25 GDPR (concetti di privacy-by-default e privacy-by-design)”

Il Responsabile del Trattamento

Art. 28

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

La nomina del responsabile deve avvenire per iscritto, con un CONTRATTO

Trattamento sotto l'autorità del titolare o del responsabile del trattamento

Art. 29
Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Chiunque agisca sotto l’autorità del titolare (compreso il responsabile) o del responsabile, che abbia accesso a dati personali non può trattare tali dati **se non è istruito in tal senso dal titolare del trattamento**.

Registri delle attività di trattamento

Art. 30

Il titolare del trattamento deve tenere (in forma scritta, anche in formato elettronico) un registro delle attività di trattamento svolte sotto la propria responsabilità.

Tale obbligo non si applica alle imprese o organizzazioni con meno di 250 dipendenti

Registri delle attività di trattamento

a meno che:

il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato

o il trattamento non sia occasionale

o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10

Registri delle attività di trattamento

Il registro del titolare contiene tutte le informazioni di cui al par. 1 dell'art. 30.

Anche i Responsabili del trattamento tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenenti le informazioni di cui al par. 2 dell'art. 30

Adozione di misure di sicurezza adeguate

Art. 32

Il Titolare e il Responsabile mettono in atto **misure tecniche e organizzative adeguate** per **garantire un livello di sicurezza adeguato al rischio**, **tenendo conto**:
dello stato dell'arte
dei costi di attuazione
della natura del trattamento
dell'oggetto del trattamento
del contesto del trattamento
delle finalità del trattamento

Nella predisposizione (o nell'aggiornamento) del sistema di trattamento, dovrà tersi conto di tali criteri, per valutare l'adeguatezza delle misure di sicurezza

Adozione di misure di sicurezza adeguate

(continua):
del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche: in special modo, dei rischi derivanti:

- dalla distruzione dei dati personali conservati o comunque trattati.
- dalla perdita dei dati personali conservati o comunque trattati.
- dalla modifica dei dati personali conservati o comunque trattati.
- dalla divulgazione non autorizzata dei dati personali conservati o comunque trattati.
- dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Tali misure debbono essere periodicamente riesaminate e, se necessario, aggiornate

Adozione di misure di sicurezza adeguate

Se del caso (alla luce dei criteri visti), tali misure tecniche e organizzative, per risultare adeguate, comprendono, tra le altre:

la **pseudonimizzazione** dei dati personali;
la **cifratura** dei dati personali;
la capacità di:

- assicurare la continua riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- 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 dati (DPIA)

L’art. 35 introduce la nozione di valutazione di impatto sulla protezione dei dati
(“DPIA”, *Data Protection Impact Assessment*, oppure “PIA”, *Privacy Impact Assessment*)

Nei casi previsti dalla norma, il titolare effettua, **prima di procedere al trattamento**, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali

Valutazione d'impatto sulla protezione dati (DPIA)

Il titolare che debba iniziare un trattamento che preveda l'uso di nuove tecnologie e **che possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche** deve **effettuare (e redigere) una valutazione d'impatto** dei trattamenti previsti sulla protezione dei dati personali.

Il rischio elevato deve essere valutato considerando la natura, l'oggetto, il contesto e le finalità del trattamento.

Data Protection Officer
(Responsabile della Protezione dei Dati)

È UNA NUOVA FIGURA

Deve essere obbligatoriamente (“sistematicamente”) designato, dal Titolare o dal Responsabile del trattamento, se:

il trattamento è effettuato da una PA

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** di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10

lo stabilisca lo stato membro in altri casi

Data Protection Officer
(Responsabile della Protezione dei Dati)

Il 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.

Il DPO può essere un dipendente del titolare o del responsabile oppure assolvere i suoi compiti in base a un contratto di servizi.

Il titolare o il responsabile pubblica i dati di contatto del DPO e li comunica all'autorità di controllo.

Data Protection Officer
(Responsabile della Protezione dei Dati)

Il DPO è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare o al responsabile nonché ai loro dipendenti in merito agli obblighi privacy;
b) sorvegliare l'osservanza delle normative privacy, nonché delle privacy policy aziendali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire pareri che gli vengano richiesti in merito alla valutazione d'impatto e sorvegliarne lo svolgimento
d) cooperare con l'autorità di controllo
e) fungere da punto di contatto per essa per questioni connesse al trattamento

Il Data Breach (la violazione dei Dati Personali)

Il titolare del trattamento deve **documentare qualsiasi violazione dei dati personali**, cioè “la violazione di sicurezza che comporti, accidentalmente o in modo illecito:

- la distruzione
- la perdita
- la modifica
- la divulgazione non autorizzata
- l’accesso

ai dati personali trasmessi, conservati o comunque trattati” (art. 4, par. 1, n. 12)

Documentare anche le circostanze relative alla violazione, le sue conseguenze e i provvedimenti adottati per porvi rimedio

Il Data Breach (la violazione dei Dati Personali)

L’art. 33 prevede l’obbligo di notificazione all’Autorità di controllo delle violazioni di dati personali, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

A meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora non venga effettuata nel termine, è ancora possibile fare la notifica oltre le 72 ore, corredata da (validi) motivi del ritardo.

Il Data Breach (la violazione dei Dati Personali)

La violazione è comunicata dal titolare **anche all'interessato** senza ritardo (ma non c'è il vincolo delle 72 ore).

In tal modo, l'interessato può prendere le precauzioni necessarie in materia.

Deve avere un linguaggio semplice e chiaro, al fine di fare comprendere all'interessato la natura della violazione

Il titolare dovrebbe anche formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi
(v. considerando n. 86)

COMUNICAZIONE AGLI INTERESSATI

La violazione **non** è comunicata all'interessato **se**:

a) il data breach **non possa presentare un rischio elevato** per i diritti e le libertà delle persone fisiche
b) sussistessero **misure tecniche e organizzative adeguate di protezione, applicate ai dati** oggetto della violazione (soprattutto cifratura e pseudonimizzazione)
c) siano **successivamente state adottate misure atte a scongiurare** il sopraggiungere di un rischio elevato
d) la comunicazione richiederebbe **sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia