SESSIONE 3

17 maggio 2018

Responsabilità e obblighi del titolare del trattamento nel Regolamento Europeo in materia di protezione dei dati personali (n. 2016/679 – di seguito «Regolamento» o «GDPR»)

Avv. Chiara Rossana Agostini

INDICE

1.

La nuova *responsabilizzazione* del titolare

Accountability e *Risk Based Approach*

1. La nuova responsabilizzazione del titolare : *accountability* e «*risk based approach*»

VECCHIA IMPOSTAZIONE: FORMALE

Nella vigenza del Codice privacy
PREVISIONE DI STANDARD MINIMI PER IL TRATTAMENTO DEI DATI

NUOVA IMPOSTAZIONE: SOSTANZIALE

Con il Regolamento
APPROCCIO PROATTIVO

1. La nuova responsabilizzazione del titolare : *accountability* e «*risk based approach*»

Accountability significa che, in forza del Regolamento, il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è stato effettuato conformemente al Regolamento nel rispetto dei principi di privacy by design e privacy by default.

In particolare, *Accountability* significa che il titolare del trattamento dev'essere in grado di dimostrare la conformità delle attività di trattamento con il Regolamento, in particolare per quanto riguarda l'efficacia delle misure tecniche e organizzative sopra menzionate (art. 5; *considerando* 77 GDPR).

1. La nuova responsabilizzazione del titolare : *accountability* e «*risk based approach*»

Quello dell'*Accountability* è un **principio di responsabilità e responsabilizzazione** per il titolare del trattamento, che deve dimostrare in modo sostanziale, secondo il grado tecnologico e organizzativo del momento, **di aver adottato tutte le procedure adeguate ed idonee ad evitare la perdita di dati** e di avere attuato misure tecniche e organizzative per assicurare la conformità al Regolamento.

Fra le procedure appena menzionate va compresa anche una verifica dell'efficacia delle misure prescelte, il riesame periodico delle stesse e il loro **aggiornamento in funzione dei cambiamenti** che avvengono in relazione alle tecnologie, ai rischi, al contesto e alle finalità del trattamento.

2.

Analisi del rischio e *Data Protection Impact Assessment*

2. Analisi del rischio e Data Protection Impact Assessment

Prima di procedere al trattamento e, in ogni caso, ad intervalli periodici, il titolare del trattamento **deve effettuare un'analisi dei rischi connessi al trattamento**, secondo quanto previsto dall'art. 24 e dal *considerando* 83 del GDPR, al fine di implementare le appropriate misure di sicurezza.

Nel valutare l'adeguato livello di sicurezza, occorre tenere conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

In base a questa iniziale valutazione dei rischi il titolare può decidere se occorre compiere una vera e propria valutazione d'impatto sulla protezione dei dati, *Data Protection Impact Assessment («DPIA»)* per determinare, in particolare, l'origine, la natura, la particolarità e la gravità del rischio.

2. Analisi del rischio e Data Protection Impact Assessment

L’esecuzione del DPIA **è prevista obbligatoriamente dal GDPR** (art. 35, considerando 84, 89, 93 e 95) quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**. In tale scenario il titolare del trattamento effettua, **prima di procedere al trattamento**, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Analisi del rischio e Data Protection Impact Assessment

Oltre alla suddetta ipotesi generale,
il titolare è tenuto ad effettuare la valutazione preventiva di impatto sulla protezione dei dati quando intenda effettuare:

↓

Art. 35.3

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** di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;

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

2. Analisi del rischio e Data Protection Impact Assessment

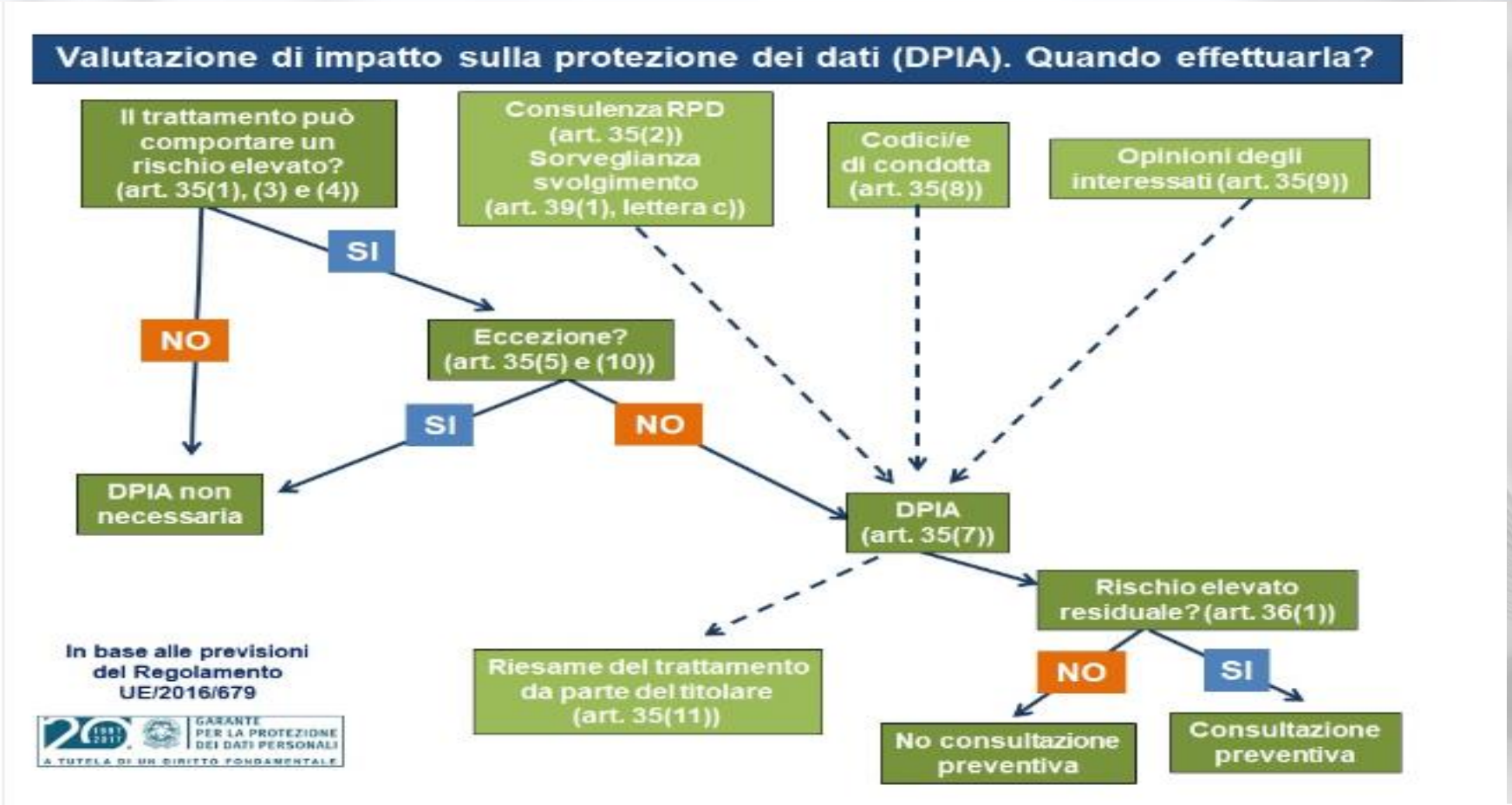
L'art. 35. 4 del Regolamento impone all'autorità di controllo (il Garante) di redigere e rendere pubblici:

a)un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1 dell'art. 35.

e, preferibilmente

b)un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati.

2. Analisi del rischio e Data Protection Impact Assessment



2. Analisi del rischio e Data Protection Impact Assessment

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

LA VALUTAZIONE PREVENTIVA DEVE CONTENERE

una valutazione dei rischi per i diritti e le libertà degli interessati di cui all'IPOTESI GENERALE (art. 35 c.1)

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 presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

3.

Il registro dei trattamenti

3. Il registro dei trattamenti

Definizione

Il Registro del trattamento è un nuovo strumento introdotto dal Regolamento Europeo per consentire alle autorità di controllo competenti di monitorare le attività di trattamento dei dati personali effettuate dal Titolare o dal Responsabile del trattamento sotto la propria responsabilità.

Forma

Il Registro del trattamento è da tenersi in forma scritta (anche in formato elettronico).

Finalità

«*Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere, un registro delle attività di trattamento effettuate sotto la sua responsabilità. Bisognerebbe obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti*».

3. Il Registro dei trattamenti

Obbligatorietà

Art. 30 del Regolamento

•La tenuta di un registro del trattamento è **obbligatoria** solo per le imprese od organizzazioni **con più di 250 dipendenti**.

•Le imprese od organizzazioni con **meno di 250 dipendenti**, invece, sono obbligate alla tenuta del Registro del trattamento solo nel caso in cui effettuino un trattamento in grado di presentare un **rischio per i diritti e le libertà dell'interessato** e, alternativamente:

-**non occasionale**;

ovvero

-**relativo a categorie particolari di dati personali** ai sensi dell'art. 9.1 del Regolamento (origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona)

ovvero

-**relativo a condanne penali**, a reati o a connesse misure di sicurezza.

3. Il registro dei trattamenti

Contenuto:

1.il nome e i **dati di contatto del titolare** del trattamento e, ove applicabile, del **contitolare** del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati («**DPO**»);

2.le **finalità** del trattamento;

3.una descrizione delle **categorie di interessati** e delle **categorie di dati** personali;

4. le **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

5. se applicabile, indicazione dei **trasferimenti di dati personali verso un paese terzo** o un'organizzazione internazionale, con identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate (decisione di adeguatezza, *privacy shield, binding corporate rules, etc.*)

6. se possibile, i **termini** ultimi previsti per la **cancellazione** delle diverse categorie di dati;

7. se possibile, una descrizione generale delle **misure di sicurezza tecniche e organizzative**.

4.

Il *Data Protection Officer*
Responsabile per la Protezione dei Dati

4. Il Data Protection Officer

Chi può essere nominato DPO?

Un **soggetto interno** alla struttura del titolare o del responsabile del trattamento (es. dipendente).

Un **soggetto esterno** alla struttura del titolare o del responsabile che opera in base a un contratto di servizi.

In quali circostanze è obbligatorio designare il DPO?

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, 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.

4. Il Data Protection Officer

compiti minimi da affidare al DPO

↓

1.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;

2.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;

3.fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

4.cooperare con l'autorità di controllo;

5.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.

4. Il Data Protection Officer

Caratteristiche e funzioni del DPO

•E’ un professionista che deve avere un ruolo aziendale (sia esso soggetto interno o esterno) con competenze giuridiche, informatiche, di risk management e di analisi dei processi

•Nell’ambito della sua attività deve osservare e supervisionare la gestione del trattamento di dati personali (e dunque la loro protezione) all’interno dell’azienda (sia essa pubblica o privata), affinché questi siano trattati nel rispetto delle normative privacy europee e domestiche

•Deve dimostrare una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all’art. 39 GDPR (vedi slide precedente.

4. Il Data Protection Officer

Il DPO e il rapporto con i suoi interlocutori:

•Il titolare e il responsabile del trattamento (che a sua volta – come anticipato – potrebbe dover nominare un suo DPO) devono assicurare **l'indipendenza e l'autonomia del DPO**, astenendosi dall'impartire istruzioni per l'esecuzione dei suoi compiti ed evitando penalizzazioni di qualsiasi tipo in relazione alle sue scelte tecniche in ambito privacy

•Gli **interessati hanno facoltà di contattare direttamente il DPO** per ogni questione riguardante il trattamento dei loro dati ed esercitare i propri diritti, in particolare i diritti di accesso, che passano attraverso il DPO indicato nell'informativa

•Il DPO deve mantenere il segreto professionale ed **astenersi dal ricoprire funzioni in conflitto** con il suo ruolo e la sua autonomia

4. Il Data Protection Officer

Comprendere quando è obbligatorio il DPO, il concetto di «larga scala»:

Il termine non è formalmente definito tra gli articoli del GDPR, il considerando 91 inquadra i trattamenti su larga scala tra quelli che «*mirano alla trattazione di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*"

4. Il Data Protection Officer

Comprendere quando è obbligatorio il DPO, il concetto di «larga scala»:

Il Gruppo di Lavoro Art. 29 (organo che riunisce i Garanti dei membri dell'UE) raccomanda di considerare i seguenti fattori per determinare se sussista «trattamento su larga scala»:

1.il numero di soggetti interessati, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

2.il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;

3.la durata, ovvero la persistenza dell'attività di trattamento;

4.la portata geografica dell'attività di trattamento.

5.dati relativi a pazienti svolto da un ospedale/struttura sanitaria;

[*segue*]

4. Il Data Protection Officer

Comprendere quando è obbligatorio il DPO, il concetto di «larga scala»:

Il Gruppo di Lavoro Art. 29 (organo che riunisce i Garanti dei membri dell'UE) raccomanda di considerare i seguenti fattori per determinare se sussista «trattamento su larga scala»:

6.dati relativi agli spostamenti di utenti servizio di trasporto pubblico;

7.dati di geolocalizzazione raccolti in tempo reale per finalità statistiche;

8.dati relativi alla clientela da parte di una compagnia assicurativa o di una banca;

9.dati personali da parte di un motore di ricerca per finalità di pubblicità/marketing;

10.dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

4. Il Data Protection Officer

Comprendere quando è obbligatorio il DPO, il concetto di «monitoraggio regolare e sistematico»

•il *considerando* 24 lo definisce come *«il monitoraggio del comportamento degli interessati ricomprende tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità e marketing*»

•possiamo ritenere «regolare» il monitoraggio (i) che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito, (ii) ricorrente o ripetuto a intervalli costanti (iii) che avviene in modo costante o a intervalli periodici.

•può considerarsi «sistematico» un monitoraggio (i) predeterminato, organizzato o metodico, (ii) che ha luogo nell'ambito di un progetto complessivo che ha come fine la raccolta dei dati, (iii) che è una distinta componente di una specifica strategia

5.

Data Breach

5. Data Breach

Cos'è?

L'articolo 4 del Regolamento definisce il Data Breach come "violazione dei dati personali", ossia la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

In tale ambito la responsabilità del titolare è duplice: (1) evitare che avvenga una violazione predisponendo e aggiornando le misure di sicurezza più e (2) in caso di violazione, adempiere tempestivamente a quanto prescritto dal Regolamento.

5. Data Breach

Gli obblighi connessi al Data Breach

Obbligo di notifica all'Autorità Garante "senza ingiustificato ritardo" e, ove possibile, **entro 72 ore ex art. 33 del Regolamento Generale sulla Data Protection**.

↓

Obbligo di **comunicazione agli interessati** quando la violazione dei dati personali **è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche**.

5. Data Breach

Contenuto della notifica

La notifica deve contenere:

•natura della violazione dei dati personali, ivi comprese le categorie e il numero di interessati nonché il tipo e il numero di record coinvolti.

•i dati di contatto del responsabile della protezione dei dati.

•descrizione delle probabili conseguenze della violazione.

•descrizione delle misure adottate o da adottare per porre rimedio alla violazione e contrastarne gli effetti negativi.

5. Data Breach

Quando non è necessario notificare all'interessato

La notifica va fatta sempre anche all'interessato con "linguaggio semplice e chiaro" salvo:

•quando il titolare abbia implementato misure tecniche e organizzative adeguate.

↓

•quando il titolare abbia successivamente adottato misure atte a scongiurare il verificarsi di rischi elevati per i diritti e le libertà degli interessati.

↓

•quando tale comunicazione richiederebbe sforzi sproporzionati, per cui può essere sostituita da una comunicazione pubblica.

5. Data Breach

Conseguenze per il titolare

Un Data Breach può generare:

- ❑Interruzione delle attività lavorative (DoS o sabotaggio);
- ❑Perdite economiche e finanziarie dirette (cause legali, crisi reputazionali o perdita di competitività)
- ❑Perdita di fiducia tra i clienti, dipendenti e investitori;
- ❑Danni fisici, inclusi danni ai propri dipendenti o clienti (es. fabbriche, aziende di trasporti, ospedali).

6.

Le misure di sicurezza

6. Le misure di sicurezza

Art. 32 GDPR

Il titolare e il responsabile del trattamento **sono tenuti a mettere in in atto misure tecniche e organizzative** adeguate per garantire un livello di sicurezza adeguato al rischio.

In particolare, devono adottare **misure di sicurezza idonee** per la difesa dei dati personali tenendo conto:
- dello stato dell'arte e dei costi di attuazione;
- della natura, del contesto e delle finalità;
- del **rischio di varia probabilità e gravità** per i diritti e le libertà delle persone fisiche.

Un aspetto essenziale è **la valutazione dei rischi**: nel valutare l'adeguato livello di sicurezza, occorre tenere conto in special modo dei rischi presentati dal trattamento **che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso**, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati

6. Le misure di sicurezza

Le misure di sicurezza adottabili compredono:

•la **pseudonimizzazione** e la *cifratura* dei dati personali;

•la capacità di assicurare su base permanente la **riservatezza, l'integrità, la disponibilità e la resilienza** dei sistemi e dei servizi di trattamento;

•la capacità di **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.

L’esito della DPIA è il punto di partenza per la scenta delle misure di sicurezza.

7.

Privacy by default

Privacy by design

7. Privacy by design – Privacy by default

Il principio di **«privacy by design»** - o di «protezione dei dati personali fin dalla progettazione» - prevede che ogni titolare o responsabile del trattamento debba tenere in considerazione, sin dalla ideazione e progettazione delle attività di trattamento che intende porre in essere, la protezione della riservatezza dei dati personali degli interessati cui il trattamento si riferisce.

Effettuare il trattamento nel rispetto della norma, minimizzando i rischi e rispettando la tutela degli interessati.

Il principio di **«privacy by default»** - o di «protezione dei dati personali «per impostazione predefinita» - prevede che ogni titolare o responsabile effettui il trattamento dei soli dati personali degli interessati nella misura e per il tempo necessari a raggiungere le specifiche finalità del trattamento, implementando, all'interno degli ambienti, dei sistemi informatici e delle infrastrutture di rete utilizzate per tale trattamento, le misure tecniche idonee a proteggere i dati personali degli interessati.

Trattare solo dati necessari per raggiungimento delle finalità del trattamento.

7. Privacy by design – Privacy by default

Il Primo Comma dell'art. 25 GDPR

Il primo paragrafo dell'art. 25 racchiude l'essenza del c.d. "*risk based approach*": il titolare del trattamento deve **progettare** (ecco il "*by design*") ed effettuare il trattamento tenendo in considerazione **i rischi per i diritti e le libertà dei soggetti interessati**. E' proprio tale valutazione iniziale che determina l'entità della responsabilità del titolare e del responsabile del trattamento, tenuto della natura, del contesto e delle finalità del trattamento.

Il Considerando 78 esplicita le caratteristiche di alcune delle misure tecniche richieste "by design" al titolare del trattamento

"Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati"

7. Privacy by design – Privacy by default

Il Secondo Comma dell'art. 25 – Privacy by Default

Chi **organizza il trattamento dei dati personali è tenuto ad implementare misure tecniche e organizzative** (anche in questo caso si tratta di accorgimenti di natura informatica e gestionale) **che garantiscano in ogni momento che il volume di dati trattati sia il più contenuto possibile,** ossia che siano trattati esclusivamente i dati personali strettamente necessari per le finalità del trattamento.

L'analisi e la definizione delle opportune misure necessarie ad assicurare costantemente la minimizzazione del trattamento **dev'essere personalizzata rispetto a tale trattamento**: vanno infatti considerati tutti gli aspetti necessari a renderlo "minimo", in particolare la qualità e quantità dei dati, l'estensione ed entità del complessivo trattamento, la durata del periodo di *retention* e il tipo di accessibilità prevista per i dati trattati.

Elemento chiave, anche in tale ambito, sarà la corretta definizione e attuazione di *policies* che consentano di verificare e documentare che l'impostazione predefinita del trattamento è idonea a ridurre il volume dei dati personali trattamenti al minimo necessario richiesto dalle finalità del trattamento.

8.

Sanzioni

8. Il nuovo sistema sanzionatorio

Artt. 50 e ss. del Regolamento

LA CORRETTA APPLICAZIONE DEL REGOLAMENTO È GARANTITA DALL'AUTORITÀ DI CONTROLLO DI OGNI STATO MEMBRO

Il Regolamento prevede espressamente che ogni autorità di controllo abbia, nell'ambito dei cd. "**poteri correttivi**", quelli di:

- infliggere **sanzioni**;
- rivolgere **avvertimenti e ammonimenti**.

Che tipo di sanzioni sono previste dal Regolamento?

↓

SOLO SANZIONI AMMINISTRATIVE PECUNIARIE (no sanzioni penali)

le sanzioni amministrative sono inflitte in funzione delle **circostanze di ogni singolo caso**, prendendo in considerazione **11 elementi tipici** previsti dall'art. 83.2.

è concessa agli Stati membri la **possibilità di prevedere** all'interno del proprio ordinamento anche delle **sanzioni di tipo penale.**

in Italia il nuovo schema di decreto prevede sanzioni penali (quelle previste nel Codice Privacy + nuove fattispecie)

8. Il nuovo sistema sanzionatorio: criteri di applicazione

1. **natura, GRAVITÀ e durata DELLA VIOLAZIONE** tenendo in considerazione la **natura, l'oggetto o a finalità del trattamento** in questione nonché il **numero di interessati lesi** dal danno e il **livello del danno da essi subito**;
2. carattere **doloso o colposo** della violazione;
3. **MISURE ADOTTATE** dal titolare del trattamento o dal responsabile del trattamento **PER ATTENUARE IL DANNO** subito dagli interessati;
4. **grado di responsabilità** del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto;
5. eventuali **precedenti violazioni pertinenti** commesse dal titolare del trattamento o dal responsabile del trattamento;
6. grado di **cooperazione con l'autorità di controllo** al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
7. **categorie di dati** personali interessate dalla violazione;
8. maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione **(data breach)**;
9. qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il **rispetto di tali provvedimenti**;
10. **l'adesione ai codici di condotta o ai meccanismi di certificazione;**
11. eventuali **altri fattori aggravanti o attenuanti applicabili** alle circostanze del caso (ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione).

8. Il nuovo sistema sanzionatorio: l'ammontare delle sanzioni

fino a 10 milioni di euro,
o per le imprese, fino al 2 % del fatturato

fino a 20 milioni di euro,
o per le imprese, fino al 4 % del fatturato

per la violazione degli:

• obblighi del titolare del trattamento e del responsabile del trattamento connessi:
- al consenso dei minori;
- ai trattamenti senza identificazione dell'interessato;
- ai principi di *accountability*, Privacy by design e by default, al Joint Controller, ai responsabili del trattamento, alla tenuta di un registro del trattamento;
- al trasferimento dei dati all'estero;

• obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

• obblighi dell'organismo di controllo a norma dell'articolo 41.4.

per la violazione:

• dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;

• dei diritti degli interessati a norma degli articoli da 12 a 22;

• dei trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;

• di qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX (artt. da 85 a 91);

• ovvero per l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo o il negato accesso.

GRAZIE

Chiara Agostini

chiara.agostini@replegal.it

www.replegal.it