Il nuovo Regolamento europeo sul trattamento dei dati personali: cosa cambia rispetto al Codice della Privacy

Roma, 16 aprile 2018

Avv. Marco Iecher

LE PRINCIPALI NOVITÀ DEL REGOLAMENTO EUROPEO

«GDPR»

- «General Data Protection Regulation» o RGPD, «regolamento generale sulla protezione dei dati». Regolamento UE **2016/679**
- Pubblicato su Gazzetta Ufficiale Europea il 4/5/2016 ed entrato in vigore il 25/5/2016, inizierà ad avere efficacia due anni dopo: il **25/5/2018**

«Self executing»

- Il regolamento è **direttamente applicabile** in tutti gli stati membri e non sono necessari atti di recepimento interni.
- Potrebbe essere adottata una normativa di raccordo
- Sostituirà la vecchia Direttiva 95/46/EC e abrogherà le norme del Codice per la protezione dei dati personali (dlgs.n. 196/2003) che risulteranno incompatibili.

Ambito applicativo

- Si applica ai **dati dei residenti nell'Unione** Europea.
- Quindi, anche se l'impresa, l'ente, l'organizzazione che tratta i dati ha sede fuori dall'Unione Europea (novità!)
- (Indipendentemente dall'ubicazione del server)

Ambito applicativo

- Si applica al **trattamento interamente o parzialmente automatizzato di dati personali** (cons. 15), non «i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici»;
- Non si applica alle attività che non sono oggetto di competenza dell'UE, come la sicurezza nazionale (cons. 16);

Ambito applicativo

- Non si applica ai trattamenti effettuati per **soli scopi personali e domestici** (cons. 18);
- Non si applica ai trattamenti effettuati dalle Autorità per scopi di **prevenzione, indagine, repressione di reati, sicurezza pubblica e politica estera** (cons. 19).

Ambito applicativo

- Non disciplina il trattamento dei dati delle **persone giuridiche** (cons. 14)
- Non si applica alle persone decedute (cons. 27)

Una nuova impostazione

- D.Lgs 169/03 → Logica **dell'adempimento**
- GDPR → Creazione di un **sistema «generale»** che tenga conto delle modalità corrette di trattamento dei dati: utilizzare i dati personali necessari per lo svolgimento dell'attività, proteggendo gli interessati

Una nuova impostazione

- Una **normativa molto flessibile**, con previsioni più «aperte» e adattabili all'evoluzione tecnologica e sociale.
- È incentrata sul dovere del titolare di **valutare i rischi** che in concreto un trattamento di dati può comportare. L'adempimento alle prescrizioni della normativa sarà conseguenza di questa valutazione.

Una nuova impostazione

- Principio dell'**accountability** («responsabilizzazione»)
- **Privacy by design** (a partire dalla progettazione)
- **Privacy by default** (per impostazione predefinita)

Di conseguenza, i titolari dovranno dotarsi di un «meccanismo» privacy che possa correttamente funzionare e soddisfare i requisiti di legge

Keep calm

- Se la vostra attività è in regola con le previsioni del D.Lgs. 196/03, ciò significa **che buona parte del lavoro è già stato portato a termine**
- La nomina del **DPO** molto probabilmente non riguarda la vostra attività
- Occorre quindi **prestare attenzione** a quanto c'è di nuovo, ma **senza** farsi prendere dal **panico**

Accountability

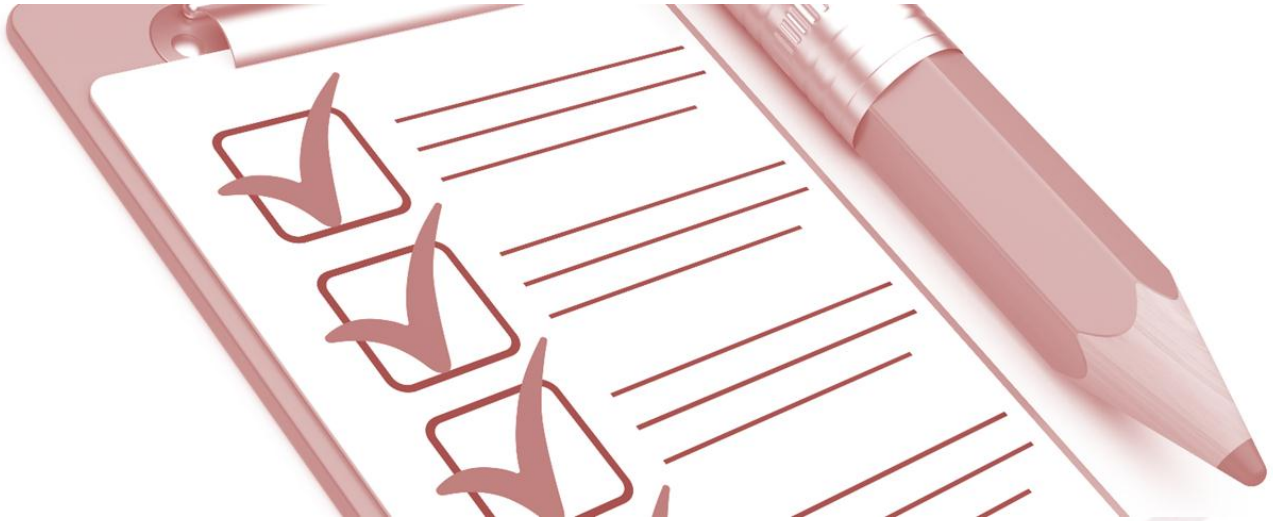
- Il regolamento pone con forza l'accento sulla "**responsabilizzazione**" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento

Privacy «by default» e «by design»

- Necessità di configurare il trattamento prevedendo **fin dall'inizio le garanzie indispensabili** "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati
- Richiede, pertanto, un'**analisi preventiva** e un **impegno applicativo** da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

Risk assessment

- Si fonda sulla **valutazione dei rischi** inerenti al trattamento: è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati.
- Tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.



GLI OBBLIGHI DEL TITOLARE

Obblighi del titolare

Il GDPR aggiunge **nuovi obblighi** e modifica in parte alcuni degli **obblighi preesistenti**.

- Informativa all'interessato
- Raccolta del consenso dell'interessato
- Procedura per l'esercizio dei diritti

Obblighi del titolare

E inoltre…

- Valutazione di impatto Privacy (DPIA)
- Registro dei trattamenti
- Nomina dei responsabili del trattamento
- Procedura in caso di «data breach»

Obblighi del titolare

E inoltre…

- Adozione di misure di sicurezza
- Nomina del DPO, se necessario

INFORMATIVA E CONSENSO

L'informativa

- Si ricorda che si tratta di un **obbligo generale** che va adempiuto prima o al massimo al momento di dare avvio alla raccolta di dati personali.
- L'informativa non è necessaria
  - In caso di **dati anonimi** (aggregati o statistici)
  - Se si trattano dati di **enti o persone giuridiche**, sebbene - attenzione - quasi sempre si finisce a trattare i dati personali delle persone fisiche che vi lavorano e dunque l'informativa torna ad essere necessaria

L'informativa

- Inoltre, non è necessaria se i dati sono trattati per attività a carattere esclusivamente **personale o domestico** (quindi, non devono poi essere comunicati o diffusi).
- Se l'interessato **già dispone di tutte le informazioni** aggiornate sul trattamento per via di una informativa resa in precedenza, non è necessario sottoporgliene una nuova.

L'informativa

- Al contrario, se dopo aver reso l'informativa le **modalità del trattamento cambiano**, sarà necessario inviarne all'interessato una **aggiornata**.

L'informativa

- In caso di dati raccolti **presso terzi**, occorrerà sottoporre l'informativa all'interessato specificando la **fonte** da cui i dati sono stati prelevati (anche se pubblici registri) e l'informativa deve essere ora resa entro un **termine «ragionevole»** e comunque dalla raccolta dell'informazione o entro la prima c**non più tardi di un mese** omunicazione del dato ad altro destinatario.

L'informativa

Secondo il GDPR, l'informativa **deve essere**

- concisa
- trasparente
- intelligibile
- facilmente accessibile
- con un linguaggio semplice e chiaro (in particolare per il caso di minori).

L'informativa

- L'informativa deve essere resa **per iscritto**, anche in forma elettronica.
- Ove richiesto dall'interessato, l'informativa è **da rendere oralmente** (purché sia comprovata con altri mezzi l'identità dell'interessato).
- Forma scritta «ad probationem»: è opportuno procurarsi una **prova dell'adempimento**.

L'informativa: contenuto

- ✓ L'identità e tutti i riferimenti di contatto del **titolare** (e, se presente, del legale rappresentante) per l'esercizio dei diritti;
- ✓ Se nominato, tutti i riferimenti di contatto del **D.P.O.**
- ✓ Quali **finalità** ha la raccolta del dato ed il trattamento

L'informativa: contenuto

- In merito alle finalità:
  - **Per ciascuna finalità** del trattamento devono essere presenti **tutte le informazioni** (è un po' come se, nel caso di finalità plurime, si redigessero altrettante informative in un unico contesto documentale);
  - **l'interessato deve essere in condizione di scegliere liberamente**, per es., di prestare il consenso al primo trattamento e non al secondo (libertà del consenso).

L'informativa: contenuto

- ✓ Quali sono le **modalità del trattamento** (modalità, cautele, misure di sicurezza): basta **una descrizione di sintesi**, senza cioè entrare in dettagli che potrebbero renderla oltremodo lunga, faticosa e incomprensibile.

L'informativa: contenuto

- ✓ Qual è la **base giuridica** del trattamento, (una norma di legge, l'adempimento di un contratto, la soddisfazione di una richiesta dell'interessato). Nel caso di sussistenza di un obbligo legale o contrattuale, può essere opportuno fornire indicazioni più precise.

L'informativa: contenuto

- ✓ Le **categorie** di persone cui i dati saranno **comunicati**
- ✓ L'eventualità che i **dati siano trasferiti a paesi extra-UE** o ad organizzazioni internazionali
- ✓ I tempi di conservazione dell'informazione

L'informativa: contenuto

- ✓ **Se l'interessato è obbligato** a fornire i dati (l'informativa deve precisare se l'interessato possa o meno **rifiutare** di fornire i dati e quali siano le **conseguenze** dell'eventuale rifiuto)

L'informativa: contenuto

✓ L'informazione dei **diritti** dell'interessato

L'interessato ha diritto:

- di **accesso** ai dati personali;
- di ottenere la **rettifica** o la **cancellazione** degli stessi o la **limitazione** del trattamento che lo riguardano;
- di **opporsi** al trattamento;
- alla **portabilità** dei dati;
- di **revocare il consenso** (salvo il trattamento serva ad adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento);
- di proporre **reclamo** all'autorità di controllo (Garante Privacy).

L'informativa: contenuto

- ✓ L'interessato deve essere informato se esiste un **processo decisionale automatizzato**, ivi inclusa la **profilazione**.

Il consenso

Secondo il considerando 32, il consenso **deve essere**

- inequivocabile;
- libero;
- specifico;
- informato;
- verificabile;
- revocabile.

Il consenso

Consenso **inequivocabile** (unambiguous nella versione inglese) vuol dire che non è necessario che sia esplicito ma può anche essere implicito (ma non tacito), purché, **non sussista alcun dubbio** che l'interessato abbia voluto comunicare il proprio consenso. Cioè deve prevedere una **chiara azione positiva** (come spuntare una casella od inserire la mail in un campo dove è specificata la finalità per la quale sarà usato il dato).

Il consenso

Il consenso deve, invece, essere **esplicito** (art. 9 GDPR) nel caso di **trattamento di dati sensibili** o nel caso di processi decisionali automatizzati (es. profilazione).

Occorre dire che la versione originaria della proposta della Commissione europea prevedeva sempre il consenso esplicito, poi si è pervenuti al compromesso attuale.

Il consenso

Il consenso deve essere **libero**, il ché significa che l'interessato deve essere in grado di operare **una scelta effettiva**, senza subire intimidazioni o raggiri, né deve subire conseguenze negative a seguito del mancato conferimento del consenso.

Ad esempio, nel caso di pubblicità commerciale, il consenso deve essere separato rispetto al consenso per la prestazione contrattuale richiesta dall'utente, perché l'utente deve avere la possibilità di ottenere la prestazione senza dover subire il ricatto di dover ricevere pubblicità commerciale.

Il consenso

Il consenso deve essere **specifico**, cioè relativo alla finalità per la quale è eseguito quel trattamento. Qualora il trattamento abbia **più finalità**, il consenso dovrebbe essere prestato per ogni finalità (Considerando 32 GDPR).

Il consenso

Il consenso deve essere **informato**, occorre cioè che l'interessato sia posto in condizioni di conoscere quali dati sono trattati, con che modalità e finalità e i diritti che gli sono attribuiti dalla legge. L'informazione si ha attraverso l'apposita informativa, di cui abbiamo già parlato.

Il consenso

Deve essere **verificabile:** non vuol dire che il consenso deve essere documentato per iscritto, né che è richiesta la forma scritta, ma si deve essere in grado di **dimostrare** che l'interessato lo ha conferito con riferimento a quello specifico trattamento.

Il consenso

Il consenso deve essere **revocabile** in qualsiasi momento, in modo semplice. Non vi è alcun obbligo di motivare la revoca, a seguito della quale il trattamento deve interrompersi (ovviamente la revoca non comporta illiceità del trattamento precedente, ma solo l'obbligo di **terminare il trattamento**), a meno che non sussista una **differente base giuridica** per continuare il trattamento.

Scadenza del consenso

Quando si raccolgono dati personali occorre informare l'interessato della **durata della conservazione** (e quindi trattamento) del dato, scaduta la quale il dato va o anonimizzato oppure cancellato.

Per questo motivo in alcuni casi potrebbe essere preferibile una base giuridica diversa dal consenso, come ad esempio i legittimi interessi del titolare del trattamento.

Consenso dei minori

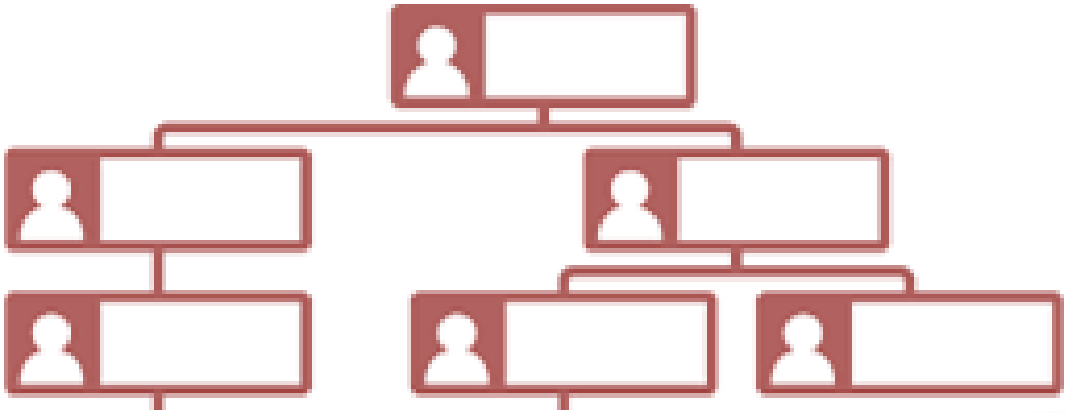
Il consenso dei minori è valido a partire dai **16 anni** di età.

Prima dei 16 anni occorre raccogliere il consenso dei **genitori** o di chi ne fa le veci.

Esonero dal consenso

L'art. 6 del GDPR prevede per il titolare **l'esonero dalla raccolta consenso** nei casi di:

- esecuzione di un **contratto**;
- adempimento di **un obbligo legale** al quale è soggetto il titolare;
- perseguimento di una finalità di **interesse pubblico**;
- tutela di un **diritto di terzi** (purché di pari rango a quello dell'interessato).



LE FIGURE SOGGETTIVE NEL GDPR

Le figure soggettive

- **Titolare**: “la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali”;
- **Responsabile:** “la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento”

Le figure soggettive

- il Responsabile per la protezione dei dati (il “Data Protection Officer” o **D.P.O.**)
- Il **destinatario dei dati**: la persona fisica o giuridica cui vengono comunicate le informazioni dell’interessato (sia privata che pubblica)
- Il **terzo:** in via residuale, chiunque non possa essere ricondotto ad alcuna delle altre categorie.

E l'«incaricato»?

- Nel Regolamento non c'è una definizione di **incaricato**, come oggi nel D.Lgs. 196, ma una figura del genere compare in alcune norme e, in ogni caso, resta vigente la disciplina in merito (ad esempio, in relazione agli atti di nomina).

Il «contitolare»

- Art. 26: la **contitolarità**. Quando “due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono da considerarsi contitolari del trattamento”.
- Potrebbe riguardare professionisti che operano in uno studio associato.

Il «contitolare»

- I vari titolari devono determinare con un **accordo** i rispettivi ruoli e le rispettive responsabilità con riferimento ai vari obblighi (informativa, consenso, esercizio dei diritti)
- L'interessato può richiedere **l'accesso** a questo accordo
- **L'esercizio dei diritti** può essere proposto dall'interessato contro uno qualunque dei contitolari.

I DIRITTI DELL'INTERESSATO

I diritti dell'interessato

- Il novero dei diritti dell'interessato è stato **ampliato**, secondo quanto disciplinato dagli artt. 12 e seguenti.
- L'interessato conserva il diritto ad essere **informato** in modo chiaro e semplice sulle caratteristiche del trattamento, ed deve essere **agevolato** nell'esercizio dei propri diritti.

I diritti dell'interessato

Inoltre, vengono specificamente disciplinati:

- Articolo 15: "**diritto di accesso dell'interessato**". l'interessato ha diritto di ottenere dal titolare **l'accesso** ai dati che lo riguardano. Inoltre ha il diritto di conoscere le **finalità** perseguite con il trattamento, i **destinatari** a cui verranno comunicati i dati, la **durata** del trattamento e le eventuali **conseguenze** di un trattamento basato sulla **profilazione**.

I diritti dell'interessato

- Articolo 16: **"diritto di rettifica e integrazione**", il diritto di ottenere dal titolare del trattamento la **rettifica** dei dati personali inesatti che lo riguardano e **l'integrazione** dei dati personali incompleti.

I diritti dell'interessato

- Articolo 17: "**diritto all'oblio**". Il GDPR introduce il diritto dell'interessato ad **ottenere la cancellazione** dei propri dati personali se **non pertinenti** o non più pertinenti, o se **inadeguati** rispetto alle finalità del trattamento, o se l'interessato abbia **revocato il proprio consenso**, o qualora i dati siano trattati in modo **illecito**.

I diritti dell'interessato

- Articolo 18: "**diritto di limitazione di trattamento**", se non sussistono gli estremi della cancellazione;
- Articolo 20: "**diritto alla portabilità**". consente all'interessato di **ricevere** i dati personali forniti a un titolare, **in un formato di uso comune** e leggibile da dispositivo informatico, e di **trasferirli** a un altro titolare del trattamento senza impedimenti.

I diritti dell'interessato

- Articolo 21: "**diritto di opposizione**", l'interessato può opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano. Il titolare del trattamento **si astiene dal trattare ulteriormente i dati** personali salvo che egli dimostri l'esistenza prevalenti motivi legittimi per procedere al trattamento.

IL DATA PROTECTION OFFICER

IL D.P.O.

- o R.P.D., «Responsabile della protezione del dati».
- È una delle più discusse **novità** del Regolamento
- È **diverso dal tradizionale «responsabile del trattamento»**, che è un soggetto nominato facoltativamente dal titolare, la cui responsabilità si differenzia secondo le funzioni specifiche che è chiamato a svolgere (responsabile della sicurezza, dell'esercizio dei diritti ecc.)

IL D.P.O.

- Il D.P.O. invece deve essere nominato **obbligatoriamente per determinate fattispecie di trattamento** (art. 37), mentre negli altri casi la nomina è solo facoltativa
- I compiti del DPO sono stabiliti dal Regolamento (art. 39)

IL D.P.O.

Art. 37: il D.P.O. deve essere nominato «**sistematicamente**» quando:

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

IL D.P.O.

b) 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**; oppure

IL D.P.O.

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

IL D.P.O.

- Svolge un ruolo **bifronte**: da un lato, rappresenta il **riferimento privilegiato dell'interessato**, costituendo il trait d'union tra quest'ultimo e il Titolare in tutte le questioni che concernono il trattamento e dall'altro svolge le **funzioni di interlocutore con l'Autorità Garante**.

IL D.P.O.

- Il DPO - che **può essere un dipendente interno** all'azienda, **un professionista esterno** o anche una **società** - è infatti coinvolto in tutte le questioni che concernono **l'adeguamento della struttura alla normativa** in materia di protezione dei dati personali, essendo a tal fine dotato di **autonomia** e **poteri decisionali**, nonché di **risorse finanziarie e umane** ad hoc.

IL D.P.O.

- Rappresenta anche il **punto di riferimento**, per **dipendenti e collaboratori**, che possono rivolgersi allo stesso per sottoporgli eventuali questioni di dubbia interpretazione o che necessitino di particolare attenzione.
- Deve poi vigilare sulla corretta osservanza della normativa, sull'adozione delle **misure** a tutela del dato, nonché sulla **sensibilizzazione** e sulla **formazione del personale**.

IL D.P.O.

- Art. 37 comma 5 indica che deve essere scelto «*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 D.P.O.

Per poter operare adeguatamente, il D.P.O. deve avere

- autonomia decisionale
- risorse economiche ed organizzative
- formazione specifica e aggiornata (art. 38 comma II).

IL D.P.O.

- Nomina **facoltativa**? Potrebbe avere senso, nell'ambito dell' «accountability»
- Il DPO, come precisato dal WP29, **non risponde personalmente** in caso di inosservanza del regolamento, ma **il titolare sanzionato potrebbe agire in regresso** su di lui

ALTRI ADEMPIMENTI

Registro dei trattamenti (art. 30)

- Espressione del principio di «**accountability**», è disciplinato dall'art. 30 del Regolamento e deve essere redatto, aggiornato e conservato dal Titolare.
- Deve indicare, tra le altre cose:
  - la **tipologia di dati** trattati;
  - La **tipologia degli interessati** coinvolti;
  - **l'ambito di comunicazione** dei dati;
  - i **termini di conservazione** dei dati;
  - Le **misure di sicurezza** adottate;
  - L'eventualità che i **dati siano trasferiti** all'estero.

Registro dei trattamenti

- Deve essere adottato da tutti i Titolari con **esclusione di imprese o organizzazioni con meno di 250 dipendenti**, a meno che il trattamento che esse effettuano possa presentare un **rischio** per i diritti e le libertà dell'interessato, il trattamento **non sia occasionale** o includa il trattamento di **dati sensibili o giudiziari.**

La Valutazione di Impatto Privacy (DPIA) (art. 35)

- Uno degli obblighi preliminari, strumentale alla valutazione del rischio.
- Esamina le **caratteristiche delle attività** di trattamento nell'ambito della struttura del Titolare (attraverso l'analisi dei processi e del loro concreto svolgimento), **valutandole alla luce dei principi cardine di necessità e proporzionalità ed i rischi** connessi ai diritti ed alle libertà degli interessati.

La Valutazione di Impatto Privacy (DPIA)

- Il GDPR definisce alcuni **criteri non tassativi** al ricorrere dei quali è obbligatorio per i Titolari procedere alla redazione. Lo è se si svolgono:
  - trattamenti automatizzati che comportino la **profilazione** dell'utente
  - trattamenti su **larga scala**, che abbiano ad oggetto **dati sensibili o giudiziari**,
  - trattamenti che si estrinsechino nella **sorveglianza sistematica** di un luogo accessibile al pubblico.

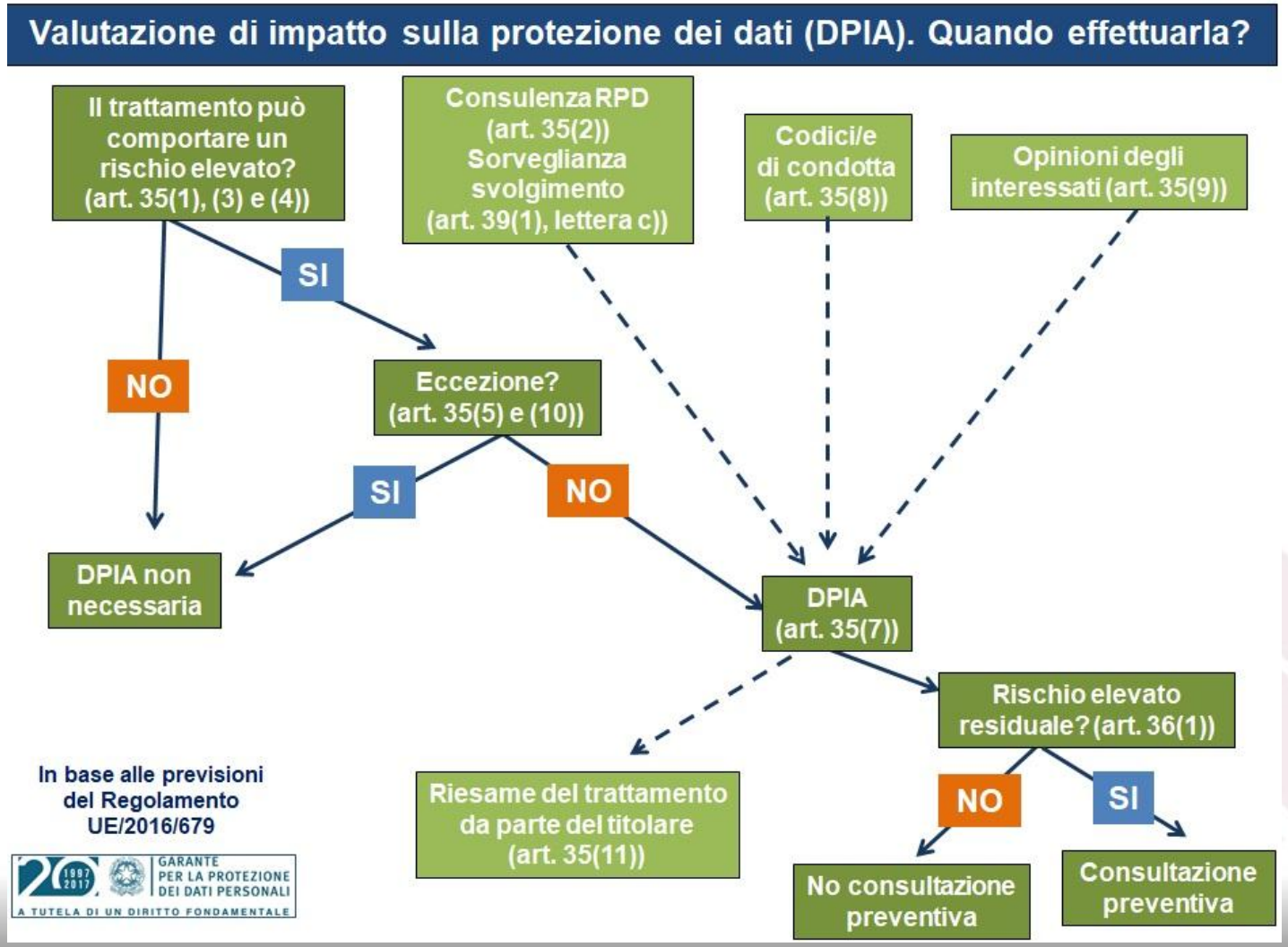
La Valutazione di Impatto Privacy (DPIA)

- Il WP29 ha redatto un parere in merito alla DPIA, ritenendo che anche sia obbligatorio procedere anche in attività a «**elevato rischio**», che sono:
  - **profilazione** degli **interessi personali**, del rendimento professionale, della **situazione economica** o dell'**ubicazione** dell'individuo;

La Valutazione di Impatto Privacy (DPIA)

- trattamenti **su larga scala**, ovvero incidenti su un numero molto elevato di soggetti in relazione al volume delle informazioni, alla durata delle operazioni di trattamento o all'estensione geografica dello stesso
- se vengano utilizzate **applicazioni tecnologiche avanzate** che abbiano un impatto incisivo sulle abitudini personali degli interessati.

La DPIA inoltre va eseguita **con cadenza periodica** e deve analizzare distintamente tutte le attività svolte


Valutazione di impatto sulla protezione dei dati (DPIA). Quando effettuarla?
Il trattamento può comportare un rischio elevato? (art. 35(1), (3) e (4))
SI
NO
Eccezione? (art. 35(5) e (10))
SI
NO
DPIA non necessaria
Consulenza RPD (art. 35(2)) Sorveglianza svolgimento (art. 39(1), lettera c))
Codici/e di condotta (art. 35(8))
Opinioni degli interessati (art. 35(9))
DPIA (art. 35(7))
Rischio elevato residuale? (art. 36(1))
NO
SI
No consultazione preventiva
Consultazione preventiva
Riesame del trattamento da parte del titolare (art. 35(11))
In base alle previsioni del Regolamento UE/2016/679
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE

La Valutazione di Impatto Privacy (DPIA)

Devono essere esaminati l'origine e la natura dei dati,

le modalità di trattamento di questi.

Devono essere adottate le conseguenziali misure di sicurezza (conosciute allo stato dell'arte),

Se il trattamento è sottoposto a notificazione, la valutazione diviene particolarmente incisiva.

Le misure di sicurezza

- **Accorgimenti tecnici** strumentali alla protezione dei dati personali oggetto di trattamento.
- L'attuale disciplina dedica una regolamentazione analitica (artt. 31-36 e l'allegato B, denominato "Disciplinare tecnico in materia di misure di sicurezza")

Le misure di sicurezza

- Nel GDPR non vengono analiticamente disciplinate ma si parla di «**misure di sicurezza adeguate**», ovvero capaci di elidere o comunque di limitare il rischio di violazione delle informazioni.
- Nell'ambito del principio di accountability, sono lasciate alla valutazione del titolare (ergo, alla sua responsabilità).

Il data breach

- Agli artt. 33 e 34 viene disciplinato quanto deve essere posto in essere dal titolare in caso di data breach.
- È previsto:
  - un **obbligo di notificazione dell'avvenuta violazione**, che deve avvenire **entro 72 ore**, con descrizione delle circostanze dell'evento e le possibili conseguenze
  - un **coordinamento con l'Autorità** di controllo.
  - quando la violazione è particolarmente grave, **l'interessato deve essere informato**.

Il data breach

- Considerando 85: *Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.*

LE SANZIONI

Le sanzioni

- L'inosservanza o l'inesatto adempimento del complesso di obblighi in materia di protezione dei dati personali configura un illecito e come tale comporta l'irrogazione di severe sanzioni di carattere **amministrativo, civile e penale**.
- Il Regolamento individua esclusivamente **criteri pecuniari massimi.**

Le sanzioni

- I parametri di gradazione delle sanzioni devono essere conseguenti:
  - alla **natura, alla gravità e alla durata** della violazione,
  - al **carattere doloso della violazione** e alle **misure adottate** per attenuare il danno subito,
  - al **grado di responsabilità** o a eventuali **precedenti** violazioni pertinenti,
  - alla maniera in cui **l'autorità di controllo ha preso conoscenza** della violazione,

Le sanzioni

- Al **rispetto dei provvedimenti** disposti nei confronti del titolare del trattamento o del responsabile del trattamento,
- all'**adesione a un codice di condotta**
- **eventuali altri fattori** aggravanti o attenuanti.

Le sanzioni

In caso di violazione degli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43 (quindi obblighi in tema di consenso dei minori, privacy by design, titolare e responsabile del trattamento, misure di sicurezza, DPO, ecc) sono previste sanzioni amministrative pecuniarie fino a **10.000.000 EUR**, o per le imprese, fino al **2 %** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

Le sanzioni

In caso di violazione dei principi fondamentali del trattamento, comprese le condizioni applicabili al consenso, di cui agli articoli 5, 6, 7 e 9; i diritti degli interessati di cui agli articoli da 12 a 22; il trasferimento di dati personali ad un destinatario in un paese terzo o ad un'organizzazione internazionale di cui agli articoli da 44 a 49;

sono previste sanzioni amministrative pecuniarie fino a **20.000.000 EUR**, o per le imprese, fino al **4 %** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Grazie per la cortese attenzione.

miecher@luiss.it