RAFFAELLA NERINI
STUDIO LEGALE

GDPR 2016/679. Disposizioni generali

Il Regolamento sulla protezione dei dati personali è entrato in vigore il 24 maggio 2016 e dovrà applicarsi dal 25 maggio 2018.

Abroga la Direttiva Europea 95/46 base del Codice Privacy Italiano (D Lgs 196/03).

Non abroga la Direttiva EU 2002/58 recepita dal Codice Privacy su comunicazioni elettroniche, marketing non richiesto, pubblicità, marketing telefonico e postale.

RAFFAELLA NERINI
STUDIO LEGALE

Il Regolamento si inserisce in un contesto normativo specifico:

General Data Protection Regulation (2016/679)

Police Directive (2016/680)

PNR-Passenger Name Record Directive (2016/681)

NIS-Network and Information Security Directive (2016/1148)

RAFFAELLA NERINI
STUDIO LEGALE

Police Directive: trattamento dati per fini di prevenzione, indagine e perseguimento reati e sicurezza pubblica

PNR Directive: dati passeggeri

NIS Directive: cybersecutity (energia, banche, trasporti, sanità, acqua, infrastrutture digitali)

RAFFAELLA NERINI
STUDIO LEGALE

Finalità

Fine (art. 1): Protezione persone fisiche, con riguardo al trattamento e alla circolazione dei dati.

Finalità:
1) protezione dati persone fisiche;
2) omogeneità normativa UE
3) rispetto della concorrenza
4) rimozione ostacoli investimenti extra UE

RAFFAELLA NERINI
STUDIO LEGALE

Il Regolamento **si applica** (art. 2): "...al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi".

Trattamento: qualsiasi operazione applicata a dati personali (*ex* raccolta, conservazione, modifica, uso, comunicazione, raffronto, cancellazione...)

Il trattamento è tale quando è oggetto di attività non causale o anche occasionale

RAFFAELLA NERINI
STUDIO LEGALE

Trattamenti esclusi:

1) scopi personali: trattamento effettuato da una persona fisica per l'esercizio di un'attività esclusivamente personale o domestica
2) Normativa extra UE: trattamento di dati per finalità estranee al diritto dell'UE
3) politica estera e sicurezza
4) sicurezza pubblica e giustizia: trattamento di dati effettuato dalle autorità competenti ai fini di prevenzione, accertamento reati, salvaguardia minacce sicurezza pubblica

RAFFAELLA NERINI
STUDIO LEGALE

Scopi personali: il Regolamento non si applica al trattamento dei dati effettuato da una persona fisica nell'ambito di attività senza connessione con un'attività commerciale o professionale.

Il rendere dati personali accessibili ad un numero illimitato di persona tramite internet on è considerato uso domestico o personale

Tale esclusione non fa venire meno l'applicazione delle norme civilistiche e penalistiche di tutela della persona (reputazione, immagine etc).

RAFFAELLA NERINI
STUDIO LEGALE

Dato personale: qualsiasi informazione concernente una persona fisica, identificata o identificabile (interessato).

Si considera *identificabile* la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come: nome, numero di identificazione, dati relativi all'ubicazione, un identificativo on line, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

(Identificativo+dato=dato personale)

RAFFAELLA NERINI
STUDIO LEGALE

Ambito di applicazione territoriale:

1) Il soggetto che tratta i dati è *stabilito* nell'UE anche se il trattamento è effettuato fuori dall'UE;

2) il soggetto *interessato si trova* nell'UE e

- il trattamento riguarda l'*offerta* di beni o la prestazione di servizi agli interessati, anche senza corrispettivo

- il trattamento riguarda il *monitoraggio* del comportamento dell'interessato all'interno della UE

RAFFAELLA NERINI
STUDIO LEGALE

Soggetti

Titolare: persona fisica/giuridica/PA che determina le finalità e i mezzi del trattamento.

Tratta il dato o perché l'interessato ha dato il suo assenso o perché la legge glielo consente, in ogni caso assume una posizione di garanzia rispetto all'interessato.

Contitolare: novità. Accordo interno

Responsabile: persona fisica/giuridica/PA che tratta i dati personali per conto del titolare.

Tratta i dati con mandato scritto e dettagliato (contratto) che contiene specifiche istruzioni sul trattamento.

Ha l'obbligo di adottare le misure di sicurezza, di assistere il titolare nelle risposta all'esercizio dei diritti degli interessati e nelle notifiche, dà informazioni utili per l'accoutability.

RAFFAELLA NERINI
STUDIO LEGALE

Incaricato: persona fisica/giuridica/PA che è autorizzata al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile.

Destinatario: persona fisica/giuridica/PA che riceve la comunicazione dei dati personali

Terzo: l'estraneo che nulla ha a che fare con il trattamento e che assumerebbe indebitamente i dati

RAFFAELLA NERINI
STUDIO LEGALE

DPO: Data Protection Officer art. 37

Nuova figura: sorta di Garante interno, denominato "Responsabile della protezione dei dati".

Il titolare e il responsabile sono obbligati alla nomina se:

- il trattamento è effettuato da un'autorità pubblica o un organismo pubblico
- le attività principali del titolare/responsabile consistono un monitoraggio regolare e sistematico degli interessati su larga scala
- le attività principali del titolare/responsabile consistono nel trattamento su larga scala di dati particolari o di dati relativi a condanne penali

RAFFAELLA NERINI
STUDIO LEGALE

Il DPO è nominato sulla base delle qualità professionali, della conoscenza specialistica della materia.

Può essere un dipendente (ma deve avere indipendenza, mezzi e risorse), oppure un esterno con contratto di servizi.

E' tenuto al segreto e alla riservatezza.

RAFFAELLA NERINI
STUDIO LEGALE

Compiti del DPO:

- informare e fornire consulenza al titolare/responsabile e ai dipendenti

- sorvegliare l'osservanza del Regolamento e delle normative anche interne sulla tutela dei dati personali, sensibilizzando e formando il personale sulla materia

- fornire, quando richiesto, un parere in merito alla valutazione d'impatto e sorvegliarne lo svolgimento

- cooperare con l'autorità di controllo

- fungere da punto di contatto con l'autorità di controllo

RAFFAELLA NERINI
STUDIO LEGALE

Regolamento: rivoluzione copernicana

Privacy by design e privacy by default: il trattamento deve essere configurato prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Prima di procedere al trattamento occorre un'analisi preventiva e un impegno applicativo che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

RAFFAELLA NERINI
STUDIO LEGALE

Privacy by design:

L'organizzazione aziendale deve essere pensata e progettata in modo che sia rispettosa del Regolamento e tuteli i diritti degli interessati.
(Giudizio di adeguatezza del trattamento)

RAFFAELLA NERINI
STUDIO LEGALE

Privacy by default:

La tutela della protezione del dato deve diventare l'impostazione predefinita.
Il titolare deve adottare le misure tecniche ed organizzative adeguate a garantire che siano trattati per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità di trattamento.

RAFFAELLA NERINI
STUDIO LEGALE

Accountability:

Principio di responsabilizzazione che richiede al titolare (e in qualche misura anche al responsabile) di mettere in atto tutte le misure tecniche ed organizzative adeguate per *garantire* ed essere in grado di *dimostrare* che il trattamento è conforme al Regolamento

RAFFAELLA NERINI
STUDIO LEGALE

Principi generali

Art. 5 Principi applicabili al trattamento (in ogni fase)

1) liceità (deve sussistere base giuridica del trattamento)

2) correttezza (rispetto sostanziale della normativa)

3) trasparenza (assicurare consapevolezza all'interessato)

4) limitazione delle finalità (gli scopi del trattamento devono essere determinati, espliciti, legittimi)

5)minimizzazione dei dati (i dati devono essere adeguati, pertinenti, limitati a quanto necessario rispetto alle finalità)

6) esattezza (i dati devono essere esatti, se necessario aggiornati)

7) limitazione della conservazione (i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un tempo non superiore alla finalità per cui sono trattati, tale termine deve essere indicato o deve essere indicato il criterio utilizzato)

8) integrità e riservatezza (devono essere trattati in modo da garantire un'adeguata sicurezza dei dati, compresa la protezione da trattamenti non autorizzati o illeciti o la perdita/distruzione/danno del dato)

RAFFAELLA NERINI
STUDIO LEGALE

Art. 6 Liceità del trattamento

Il trattamento è lecito solo e nella misura in cui ricorre almeno una delle seguenti condizioni:

1) consenso (espresso dall'interessato per una o più finalità)
2) contratto (il trattamento è necessario per l'esecuzione di un contratto – o misure precontrattuali - di cui l'interessato è parte)
3) obbligo legale (il trattamento è necessario per adempiere ad un obbligo legale cui è soggetto il titolare)

RAFFAELLA NERINI
STUDIO LEGALE

4) salvaguardia interessi vitali (il trattamento è necessario per la salvaguardia di interessi vitali dell'interessato o di altra persona fisica)

5) compiti di interesse pubblico o connessi all'esercizio di pubblici poteri (il trattamento è necessario per … di cui è investito il titolare)

6) legittimo interesse del titolare (il trattamento è necessario epr il perseguimento del … o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato)

RAFFAELLA NERINI
STUDIO LEGALE

Art. 9 Liceità per dati particolari

E' *vietato* trattare dati personali che:

1) rivelino:
   - l'origine razziale o etnica
   - le opinioni politiche
   - le convinzioni religiose o filosofiche
   - l'appartenenza sindacale
2) dati genetici
3) dati biometrici
4) dati relativi alla salute
5) dati relativi alla vita sessuale o all'orientamento sessuale della persona

RAFFAELLA NERINI
STUDIO LEGALE

Cosa si intende per:

- Dati genetici: dati relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni uniche sulla fisiologia o sulla salute

- Dati biometrici: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono l'identificazione univoca

- Dati relativi alla salute: dati personali relativi alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria che rivelano informazioni sullo stato di salute

RAFFAELLA NERINI
STUDIO LEGALE

Il trattamento è comunque ammesso se:

1) l'interessato ha prestato il proprio *consenso ESPLICITO*;
2) trattamento necessario per assolvere obblighi o esercitare diritti del titolare/interessato in materia di *diritto del lavoro e sicurezza sociale*
3) trattamento necessario per tutelare un *interesse vitale* dell'interessato o di altra persona fisica impossibilitata a prestare consenso
4) effettuato da una organizzazione senza scopo di lucro (*onlus*) per il trattamento dei propri membri o dei soggetto che hanno regolari contatti con l'ente

5) il trattamento riguarda dati personali resi *manifestamente pubblici* dall'interessato
6) il trattamento è necessario per accertare, esercitare, difendere un *diritto in sede giudiziaria*
7) il trattamento è necessario per motivi di *interesse pubblico*
8) il trattamento è necessario per finalità di *medicina preventiva o del lavoro*, valutazione della capacità lavorativa, gestione sei sistemi e servizi sanitari e sociali e devono essere trattati direttamente o sotto la responsabilità di un professionista soggetto al segreto professionale
9) il trattamento è necessario per motivi di interesse pubblico nel settore della *sanità pubblica*
10) il trattamento è necessario per fini di *archiviazione* nel pubblico interesse, di *ricerca* scientifica o storica o *statistica*

RAFFAELLA NERINI
STUDIO LEGALE

Consenso:

Il consenso è un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione *libera*, *specifica*, *informata* e *inequivocabile* di accettare il trattamento dei dati personali che lo riguardano (considerando 32)

RAFFAELLA NERINI
STUDIO LEGALE

Ne consegue che:

1) deve essere prestato per ogni finalità

2) la dichiarazione deve essere predisposta in modo chiaro e in forma comprensibile

3) la dichiarazione deve indicare almeno il titolare e la finalità per cui è prestato il consenso

4) l'interessato può revocare il consenso in ogni momento e deve essere informato di tale diritto

RAFFAELLA NERINI
STUDIO LEGALE

Principio di trasparenza

Trasparenza dell'organizzazione e delle attività, ovvero delle modalità e delle finalità e dell'esercizio dei diritti dell'interessato.

Si concretizza in:
1) dovere di informazione
2) identificazione dei soggetti che trattano i dati
3) identificazione dei mezzi usati
4) assistenza per il rintraccio dei dati inoltrati verso i destinatari
5) comunicazione delle violazioni dei dati, ulteriore rispetto a quelle obbligatorie
6) pubblicazione della valutazione di impatto privacy (buona prassi)

RAFFAELLA NERINI
STUDIO LEGALE

Novità

- Informazione su nuovi diritti (oblio, limitazione, portabilità, trattamento umano per trattamenti automatizzati/profilazione)

- tempi di risposta alle istanze di trasparenza (30 gg)

- obbligatoria informativa sui motivi per cui non viene evasa una richiesta di esercizio dei diritti

- obbligatoria informativa sui ricorsi amministrativi e giurisdizionali

- possibilità di abbinare informazioni discorsive e grafiche

RAFFAELLA NERINI
STUDIO LEGALE

L' Informativa

Il titolare del trattamento deve fornire all'interessato una serie di informazioni:

- nel momento in cui i dati sono ottenuti, se la raccolta avviene presso l'interessato
- entro un termine ragionevole (max 1 mese), se i dati non sono stati ottenuti presso l'interessato
- al più tardi al momento della prima comunicazione se i dati sono destinati alla comunicazione con l'interessato
- non oltre la prima comunicazione dei dati, se è prevista la loro comunicazione ad altro destinatario

RAFFAELLA NERINI
STUDIO LEGALE

Contenuti:

I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14 del Regolamento e in parte sono più ampi rispetto al Codice Privacy

Differenti contenuti:

1) obbligo di fornire i dati di contatto del DPO
2) mancata indicazione espressa dell'obbligo di tenere a disposizione dell'interessato l'elenco dei responsabili del trattamento
3) mancata indicazione dell'obbligo di indicare il responsabile del trattamento per il riscontro all'interessato in caso di esercizio dei diritti

RAFFAELLA NERINI
STUDIO LEGALE

4) mancata indicazione espressa dell'obbligo di indicare le modalità del trattamento
5) obbligo di indicazione della base giuridica del trattamento
6) obbligo di indicazione del legittimo interesse ad effettuare il trattamento (se condizione di liceità)
7) obbligo di indicazione espressa della possibilità del trasferimento all'estero nonché delle relative condizioni legittimanti
8) obbligo di indicazione del periodo di conservazione dei dati
9) obbligo di indicazione espressa della possibilità di revoca del consenso
10) obbligo di indicazione espressa della possibilità di reclamo all'autorità di controllo
11) obbligo di indicazione espressa delle notizie sui trattamenti automatizzati

Forma:

L'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 un'informativa idonea.

E' data, in linea di principio, per iscritto e preferibilmente in formato elettronico.

Il Regolamento ammette l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo in combinazione con l'informativa estesa (definite prossimamente dalla Commissione Europea)

RAFFAELLA NERINI
STUDIO LEGALE

Diritti degli interessati

Trasparenza e modalità art. 12

Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato e fornisce le informazioni dovute *senza giustificato ritardo* e comunque al più tardi *entro un mese* dal ricevimento della richiesta stessa. Tale termine può essere *prorogato di due mese*, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare informa l'interessato di tale proroga e dei motivi del ritardo entro un mese dal ricevimento della richiesta.

Se *non ottempera* alla richiesta, il titolare lo informa senza ritardo e al più tardi entro un mese, dei motivi dell'inottemperanza e della possibilità di proporre reclamo al Garante o reclamo giurisdizionale.

Se le richieste sono manifestamente infondate/ripetitive/eccessive il titolare può addebitare un contributo spese o rifiutarsi di rispondere.

RAFFAELLA NERINI
STUDIO LEGALE

Diritto di accesso art. 15

L'interessato ha il diritto di sapere *se* è in corso un trattamento di suoi dati personali, di avere una *copia* dei dati e ha diritto di *sapere*:

1) le finalità del trattamento
2) le categorie di dati personali
3) i destinatari o le categorie di destinatari
4) se i destinatari sono di Paesi terzi o organizzazioni internazionali
5) il periodo di conservazione dei dati oppure i criteri utilizzati
6) l'esistenza del diritto di chiedere la rettifica / cancellazione / limitazione / opposizione
7) diritto di proporre reclamo ad un'autorità di controllo
8) se dati non raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine
9) l'esistenza di un processo decisionale automatizzato / profilazione e informazioni sulla logica utilizzata, le conseguenze di tale trattamento per l'interessato

RAFFAELLA NERINI
STUDIO LEGALE

Diritto di rettifica art. 16

L'interessato ha il diritto di ottenere dal titolare la rettifica dei dati personali inesatti che lo riguardano oppure l'integrazione di detti dati, senza ingiustificato ritardo.

RAFFAELLA NERINI
STUDIO LEGALE

Limitazione del trattamento art. 18

Possibilità di imporre una restrizione (limitazione) al trattamento dei dati (*ex* sola conservazione)

Quando:

1) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare per verificare l'esattezza dei dati personali
2) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede ne sia limitato l'utilizzo
3) benché il titolare non ne abbia più bisogno, i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria
4) l'interessato si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare rispetto ai diritti dell'interessato

Conseguenze:

Se il trattamento è limitato, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziari oppure per tutelare i diritti di un'altra persona fisica o giuridica, o per motivi di interesse pubblico.

L'interessato che ha ottenuto la limitazione del trattamento è informato dal titolare prima che la limitazione sia revocata.

RAFFAELLA NERINI
STUDIO LEGALE

Diritto di opposizione art. 21

L'interessato ha diritti di opporsi al trattamento quando:

A) in ogni momento, per motivi connessi alla sua situazione particolare, in caso di trattamento dei dati personali che lo riguardano effettuati per motivi di interesse pubblico o di interesse legittimo del titolare.

Il titolare deve astenersi dal trattamento salvo che dimostri l'esistenza di motivi legittimi cogenti oppure che debba accertare/difendere/esercitare un diritto in sede giudiziaria

B) in qualsiasi momento in caso di trattamento dei dati per finalità di marketing diretto, compresa la profilazione.

Il titolare deve cessare il trattamento per tali finalità.

C) in caso di trattamento a fini di ricerca scientifica, storica, statistica, per motivi connessi alla sua situazione particolare, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

RAFFAELLA NERINI
STUDIO LEGALE

Diritto alla cancellazione o all'oblio art. 17

L'interessato ha il diritto di ottenere dal titolare del trattamento le cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare ha l'obbligo di cancellarli se:

1) i dati personali non sono più necessari rispetto alle finalità
2) l'interessato revoca il consenso, se non sussista altro fondamento giuridico al trattamento
3) l'interessato si oppone al trattamento e non sussiste motivo legittimo prevalente
4) i dati sono trattati illecitamente
5) i dati devono essere cancellati per adempiere ad un obbligo legale
6) dati raccolti su minori per offerta servizi della società di informazione

RAFFAELLA NERINI
STUDIO LEGALE

Il titolare se ha reso pubblici dati personali ed è obbligato a cancellarli, adotta le misure ragionevoli per *informare* i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi *link*, copia o riproduzione dei suoi dati personali.

Eccezione al diritto il trattamento necessario per:

- esercizio diritto alla libertà di espressione e informazione
- adempimento obbligo legale
- motivi di interesse pubblico nella sanità pubblica
- archiviazione per pubblico interesse, ricerca storica, statistica
- accertamento/esercizio/difesa di un diritto in sede giudiziaria

RAFFAELLA NERINI
STUDIO LEGALE

Diritto alla portabilità dei dati art. 20

L'interessato ha 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 e ha il diritto di *trasmettere* tali dati ad un altro titolare senza impedimenti se:

- il trattamento si basa sul consenso
- è effettuato con mezzi automatizzati

Se tecnicamente possibile, l'interessato ha diritto alla trasmissione diretta dei dati da un titolare ad un altro.

Eccezione: interesse pubblico e pubblici poteri del titolare

RAFFAELLA NERINI
STUDIO LEGALE

Processo decisionale automatizzato, compresa la profilazione art. 22

L'interessato ha il diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona.

RAFFAELLA NERINI
STUDIO LEGALE

Eccezioni:

- la decisione automatizzata è necessaria per la conclusione o l'esecuzione di un contratto
- la decisione automatizzata è autorizzata dal diritto UE o del singolo stato
- la decisione automatizzata si basa sul consenso esplicito dell'interessato.

Il titolare deve allora adottare misure appropriate per la tutela dei diritti, delle libertà e degli interessi legittimi dell'interessato e riconoscere almeno il diritto dello stesso di ottenere un intervento umano da parte del titolare, il diritto di esprimere la propria opinione e contestare la decisione

RAFFAELLA NERINI
STUDIO LEGALE

Sicurezza dati personali art. 32

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

Modalità:
- pseudonimizzazione e cifratura dati
- capacità di assicurare riservatezza/integrità/disponibilità dei sistemi
- capacità di ripristinare tempestivamente disponibilità e accesso ai dati
- procedura per testare regolarmente l'efficacia delle misure adottate

RAFFAELLA NERINI
STUDIO LEGALE

Pseudonimizzazione:

vengono sostituiti dati identificativi con un valore surrogato (token).

Il data set che rende di nuovo identificabili i dati deve rimanere separato

Come generare valori surrogati?

- Crittografia (chiave separata conosciuta solo dal controllore)
- funzioni hash (valore nuovo che si attribuisce al dato)
- funzioni keyed-hash (crittografia+hash)

RAFFAELLA NERINI
STUDIO LEGALE

Data breach artt. 33 e 34

La violazione dei dati personali è definita all'art. 4 come 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.

Si tratta di un evento che va gestito e affrontato subito, al fine di evitare danni maggiori e non deve essere celato.

Il titolare in caso di violazione deve **notificare** la violazione al Garante, senza giustificato ritardo, e, ove possibile, entro 72 ore (altrimenti motivi ritardo), a meno che sia improbabile che la violazione presenti *rischi per i diritti e le libertà* delle persone fisiche (*se rischio elevato*: comunicata all'interessato)

Il responsabile informa il titolare senza ingiustificato ritardo della violazione

La notifica deve **contenere** almeno:
- la descrizione della natura della violazione (categorie e numero interessati)
- nomi e dati di contratto del DPO o di altro soggetto per avere maggiori informazioni
- descrizione delle probabili conseguenze
- descrizione delle misure adottare per porre rimedio o attenuare i possibili effetti negativi

Qualora tali informazioni non sia possibile fornirle contestualmente, saranno fornite in fasi successive senza ingiustificato ritardo

Ogni violazione, le sue conseguenze e i provvedimenti adottati devono essere documentati.

RAFFAELLA NERINI
STUDIO LEGALE

Valutazione di impatto art. 35

Quando un trattamento può presentare un *rischio elevato* per i diritti e le libertà della persone fisiche, il titolare, prima di procedere al trattamento, deve effettuare una valutazione dell'impatto dei trattamenti sulla protezione dei dati personali (consultandosi con DPO).

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

RAFFAELLA NERINI
STUDIO LEGALE

La valutazione è sempre richiesta quando:

1) trattamento automatizzato compresa la profilazione, sul quale si fondano le decisioni che hanno effetti giuridici o incidono significativamente sull'interessato

2) trattamento su larga scala di dati particolari o dati penali

3) sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Altri casi saranno previsti dal Garante.

RAFFAELLA NERINI
STUDIO LEGALE

La valutazione contiene almeno:

- la descrizione sistematica dei trattamenti previsti, delle finalità, l'interesse legittimo se sussistente del titolare
- 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 e dimostrare il rispetto della normativa (garanzie, misure di sicurezza, meccanismi di tutela).

RAFFAELLA NERINI
STUDIO LEGALE

Registro dei trattamenti art. 30

Censimento dei trattamenti per titolare e responsabile.

Contenuto: dati titolare/responsabile, finalità,destinatari, categorie dati, trasferimenti estero, termine trattamento, misure tecniche ed organizzative.

Obbligatorio:
- Imprese con > 250 dipendenti
- Imprese con < 250 dip. ma rischio per diritti e libertà, trattamento non occasionale o trattamento dati particolari o penali

RAFFAELLA NERINI
STUDIO LEGALE

CODICI DI CONDOTTA E CERTIFICAZIONE

(ARTT. 40-42)

Le associazioni e gli altri organismi rappresentanti le categorie di titolari/responsabili possono elaborare Codici di condotta destinati a contribuire alla corretta applicazione del Regolamento (minori, raccolta dati, pseudonimizzazione, informazione, misure tecniche, procedure etc).

Conseguenza dell'adesione: graduazione sanzione amm.va e non esclusione profili di responsabilità.

Certificazione/sigilli/marchi con lo scopo di dimostrare la conformità al Regolamento (tre anni): non esime da controllo e responsabilità.

RAFFAELLA NERINI
STUDIO LEGALE

TRASFERIMENTO DATI VERSO PAESI TERZI artt. 44-50

Presupposti:

a) decisione di adeguatezza (pronuncia della Commissione di garanzie adeguate per quel paese)

b) condizioni di adeguatezza (strumenti vincolanti tra autorità pubbliche, norme vincolanti d'impresa, clausole tipo adottate dalla Commissione, codice di condotta con impegno vincolante a tutelare i diritti degli interessati, certificazione e impegno)

c) altre ipotesi (consenso espresso interessato, necessario esecuzione contratto, interesse pubblico, diritti sede giudiziaria, interessi vitali, registro pubblico)

RAFFAELLA NERINI
STUDIO LEGALE

AUTORITA' CAPOFILA e SPORTELLO UNICO

Se il trattamento si svolge:
a) in più stabilimenti del titolare/responsabile in diversi stati UE
b) in un unico stabilimento in UE, ma incide in modo sostanziale si interessati in più stati UE

Per garantire un'interpretazione e applicazione uniforme del regolamento, si prevede che la decisione sia presa di concerto con le Autorità interessate

Autorità Capofila (art. 56): è quella dello stabilimento principale e coordina ogni attività attraverso il coinvolgimento delle altre A. interessate.
Presenta un progetto di decisione e lo comunica alle altre A. che possono sollevare obiezioni (accolte/Board)

RAFFAELLA NERINI
STUDIO LEGALE

SANZIONI AMMINISTRATIVE PECUNIARIE

La sanzione deve essere “effettiva, proporzionata e dissuasiva”, adattata al caso concreto.

Fino a 10milioni o, per le imprese, fino al 2% del fatturato
(principio di minimizzazione, nomina responsabile sul territorio, mansioni e resp del responsabile e contitolare, registro attività del trattamento, cooperazione Autorità, adozione misure di sicurezza adeguate, data breach, designazione DPO)

Fino a 20 milioni o, per le imprese, fino al 4% del fatturato
(principio di liceità, presupposti di legittimità, consenso, revoca, diritti interessato, trasferimenti estero, obblighi Autorità)

RAFFAELLA NERINI
STUDIO LEGALE

Cosa occorre fare

- **revisione dei processi di trattamento** di dati personali al fine di verificare la *compliance (*privacy by design e by default);
- **revisionare** i meccanismi di **raccolta del consenso** e relative **informative***;*
- predisporre meccanismi di **risposta alle richieste** dell'interessato;
- predisporre procedure e formulari per **data breach**;
- eventuale nomina **DPO**;
- predisporre i **registri delle attività di trattamento**;
- **conservare i documenti** che giustificano le scelte privacy per accountability;
- **valutazione del rischio** e se del caso di **impatto**