Il nuovo regolamento UE in materia di protezione dei dati personali

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

La valutazione d'impatto sui dati personali

Responsabilizzazione/accountability

- Il Regolamento promuove l'adozione di approcci e politiche che tengano conto del rischio che un trattamento di dati personali può comportare
- assicurare la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema "*privacy by design*".
- Comportamenti che consentano di prevenire possibili problematiche: ad esempio, l'obbligo per i titolari/responsabili di condurre una valutazione di impatto prima di procedere ad un (nuovo) trattamento, sentendo l'Autorità garante in caso di dubbi, o di nominare in alcuni casi un "Responsabile della protezione dati" (ovvero il "Data Protection Officer") per assicurare una gestione corretta e proattiva dei dati personali trattati.
- Sono eliminati alcuni oneri considerati puramente burocratici quali la notifica dei trattamenti all'Autorità garante, o l'obbligo di ottenere l'autorizzazione dell'Autorità garante per i trattamenti considerati "a rischio" (purché sia condotta la valutazione di impatto e si consulti l'Autorità in caso di dubbi).

- Il Regolamento promuove il ricorso a codici deontologici da parte di associazioni di categoria e altri soggetti, sottoposti all'approvazione delle DPA ed eventualmente della Commissione (in tal caso, il codice deontologico avrà applicazione nell'intera UE).
- Il Regolamento introduce la possibilità per il titolare di far certificare i propri trattamenti, in misura parziale o totale, anche ai fini di trasferimenti di dati in Paesi terzi; la certificazione può essere rilasciata da un soggetto a ciò abilitato ovvero dall'Autorità garante.
- I Garanti dovranno tenere conto dell'adesione a codici deontologici e/o schemi di certificazione nel valutare eventuali violazioni del Regolamento da parte di un titolare e, più in generale, nell'analizzare i risultati della valutazione di impatto condotta da un titolare.

Linee guida adottate wp29

- RPD (responsabile protezione dati)
- Portabilità
- Autorità capofila
- Consenso
- Data breach notification
- profilazione

il rischio inerente al trattamento

- rischio di impatti negativi sulle libertà e i diritti degli interessati (considerando 75-77);
- tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (artt. 35-36)
- 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

- All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale;

- l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

L'intervento delle autorità di controllo

- si collocherà successivamente alle determinazioni assunte autonomamente dal titolare (abolizione di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto prior checking (art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/ responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia.

Comitato europeo della protezione dei dati

- Alle autorità di controllo, e al "Comitato europeo della protezione dei dati" (EDPB) spetterà di garantire uniformità di approccio e fornire ausili interpretativi e analitici.
- il Comitato dovrà produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse

Le linee guida

- Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione, aiutano i titolari del trattamento non soltanto a rispettare i requisiti del RGPD, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24). La valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità.

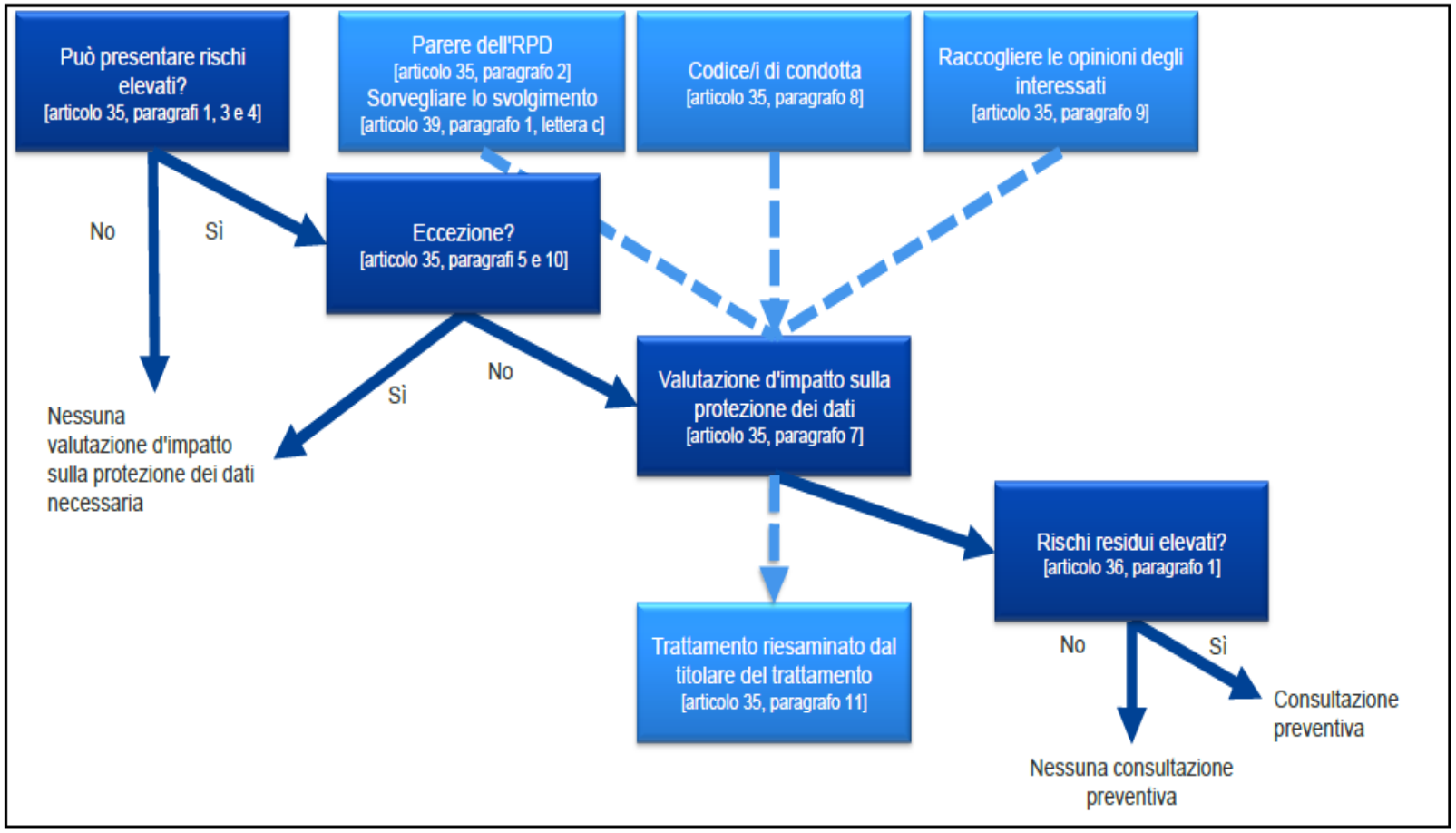
- non vi è una definizione di valutazione d'impatto ma il suo contenuto minimo è specificato dall'articolo 35, paragrafo 7:
- "a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
- d) 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";

- significato e il suo ruolo sono chiariti dal considerando 84 : "qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio".

I diritti e le libertà delle persone fisiche

- L'articolo 35 fa riferimento al possibile rischio elevato "per i diritti e le libertà delle persone fisiche".
- Il gruppo articolo 29 sulla protezione: il riferimento a "diritti e libertà" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.

La figura che segue illustra i principi fondamentali relativi alla valutazione d'impatto sulla protezione dei dati di cui al regolamento generale sulla protezione dei dati:



- Una valutazione d'impatto sulla protezione dei dati può riguardare una singola operazione di trattamento dei dati. Tuttavia, l'articolo 35, paragrafo 1, indica che "[u]na singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".
- Si può ricorrere a una singola valutazione d'impatto sulla protezione dei dati nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi, es. si utilizza una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità

Quando fare una PIA

- L'articolo 35, paragrafo 3, fornisce alcuni esempi di casi nei quali un trattamento "possa presentare rischi elevati":
- "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 fisiche12;
- 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 1013; o
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".

i nove criteri

1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato«
2. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente (considerando 71 e 91)

3. monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (articolo 35, paragrafo 3, lettera c))

4. dati sensibili o dati aventi carattere altamente personale

6. creazione di corrispondenze o combinazione di insiemi di dati,

7. dati relativi a interessati vulnerabili (considerando 75)

8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative

9. quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (articolo 22 e considerando 91)

5. trattamento di dati su larga scala: non vi è definizione della nozione di "su larga scala", tuttavia vi è un orientamento in merito al considerando 91. Il WP29 raccomanda di tenere conto dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

a. *il numero di soggetti interessati dal trattamento*, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

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

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

d. *la portata geografica* dell'attività di trattamento;

- il WP29 ritiene che maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati.
- In alcuni casi, un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno di questi criteri richieda una valutazione d'impatto sulla protezione dei dati.
- Per contro, un trattamento può corrispondere ai casi di cui sopra ed essere comunque considerato dal titolare del trattamento un trattamento tale da non "presentare un rischio elevato". In tali casi il titolare del trattamento deve giustificare e documentare i motivi che lo hanno spinto a non effettuare una valutazione d'impatto.

- L’obbligo di svolgere una valutazione d'impatto si applica alle operazioni di trattamento esistenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche e per le quali vi è stata una variazione dei rischi, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

- La PIA va effettuata "prima del trattamento" (articolo 35, paragrafi 1 e 10, considerando 90 e 93)23. Ciò è coerente con i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita (articolo 25 e considerando 78). La valutazione d'impatto sulla protezione dei dati va considerata come uno strumento atto a contribuire al processo decisionale in materia di trattamento.

- Realizzare una valutazione d'impatto sulla protezione dei dati è un processo continuo, non un esercizio una tantum.
- Al titolare del trattamento spetta assicurare che la valutazione d'impatto sulla protezione dei dati sia eseguita (articolo 35, paragrafo 2). La valutazione d'impatto sulla protezione dei dati può essere effettuata da qualcun altro, all'interno o all'esterno dell'organizzazione, tuttavia al titolare del trattamento spetta la responsabilità ultima per tale compito

La PIA e il RPD

- il titolare del trattamento deve consultarsi con il responsabile della protezione dei dati (RPD), qualora ne sia designato uno (articolo 35, paragrafo 2) e il parere ricevuto, così come le decisioni prese dal titolare del trattamento, debbano essere documentate all'interno della valutazione d'impatto sulla protezione dei dati. Il responsabile della protezione dei dati deve altresì sorvegliare lo svolgimento della valutazione d'impatto sulla protezione dei dati (articolo 39, paragrafo 1, lettera c)).

Caratteristiche minime di una valutazione d'impatto (articolo 35, paragrafo 7, e considerando 84 e 90)

- "una descrizione dei trattamenti previsti e delle finalità del trattamento";
- - "una valutazione della necessità e proporzionalità dei trattamenti";
- - "una valutazione dei rischi per i diritti e le libertà degli interessati";
- - "le misure previste per:
- o "affrontare i rischi";
- o "dimostrare la conformità al presente regolamento".


Descrizione del trattamento previsto
Valutazione della necessità e della proporzionalità
Misure previste per dimostrare la conformità
Valutazione dei rischi per i diritti e le libertà
Misure previste per affrontare i rischi
Documentazione
Monitoraggio e riesame

- Nel valutare l'impatto di un trattamento va tenuto conto (articolo 35, paragrafo 8) del rispetto di un **codice di condotta** (articolo 40). Ciò può essere utile per dimostrare che sono state scelte o messe in atto misure adeguate, a condizione che il codice di condotta sia adeguato all'operazione di trattamento interessata. Devono essere presi in considerazione anche **certificazioni**, sigilli e marchi al fine di dimostrare la conformità rispetto al RGPD dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento (articolo 42), nonché rispetto alle norme vincolanti d'impresa

Consultazione dell’Autorità.

- spetta al titolare del trattamento valutare i rischi per i diritti e le libertà degli interessati e individuare le misure previste per attenuare tali rischi a un livello accettabile e per dimostrare la conformità rispetto al regolamento generale sulla protezione dei dati (articolo 35, paragrafo 7).
- Se il titolare non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) è necessario consultare l'autorità di controllo30.