

Data Protection Impact Assessment (DPIA)

**VALUTAZIONE DI
IMPATTO**



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Valutazione d'impatto sulla protezione dei dati (DPIA)

Elenco delle tipologie di trattamenti soggetti
al requisito di una valutazione d'impatto



- Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679*



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Scheda aggiornata in base alla
versione delle Linee guida del
WP29 emendata e adottata
il 4 ottobre 2017

Valutazione di impatto sulla protezione dei dati (DPIA) – Art. 35 del Regolamento UE/2016/679

COSA È?

È una procedura prevista dall'**articolo 35 del Regolamento UE/2016/679 (RGPD)** che mira a descrivere un trattamento di dati per **valutarne la necessità e la proporzionalità nonché i relativi rischi**, allo scopo di approntare misure idonee ad affrontarli. Una DPIA **può riguardare un singolo trattamento oppure più trattamenti** che presentano **analogie** in termini di natura, ambito, contesto, finalità e rischi.

PERCHÉ?

La DPIA è uno strumento importante in termini di responsabilizzazione (*accountability*) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, **la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali**. Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego **per tutti i trattamenti, e non solo** nei casi in cui il Regolamento la prescrive come obbligatoria.

IN CHE MOMENTO?

La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, **ripetendo la valutazione a intervalli regolari**.

CHI?

La **responsabilità** della DPIA spetta al **titolare**, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora** lo svolgimento **consultandosi** con il **responsabile della protezione dei dati** (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi** (*Chief Information Security Officer, CISO*) e del **responsabile IT**.

QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche.

Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:

- trattamenti valutativi o di *scoring*, compresa la profilazione;
 - decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
 - monitoraggio sistematico (es: videosorveglianza);
 - trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
 - trattamenti di dati personali su larga scala;
 - combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
 - dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
 - utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
 - trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).
- La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON è necessaria** per i trattamenti che:

- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento. Per un quadro completo: www.garanteprivacy.it/regolamentoue



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

***CHIARIMENTO INTERPRETATIVO**

[ALLEGATO 1 AL PROVVEDIMENTO N. 467 DELL'11 OTTOBRE 2018 \[doc. web n. 9058979\]](#)

(Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018)

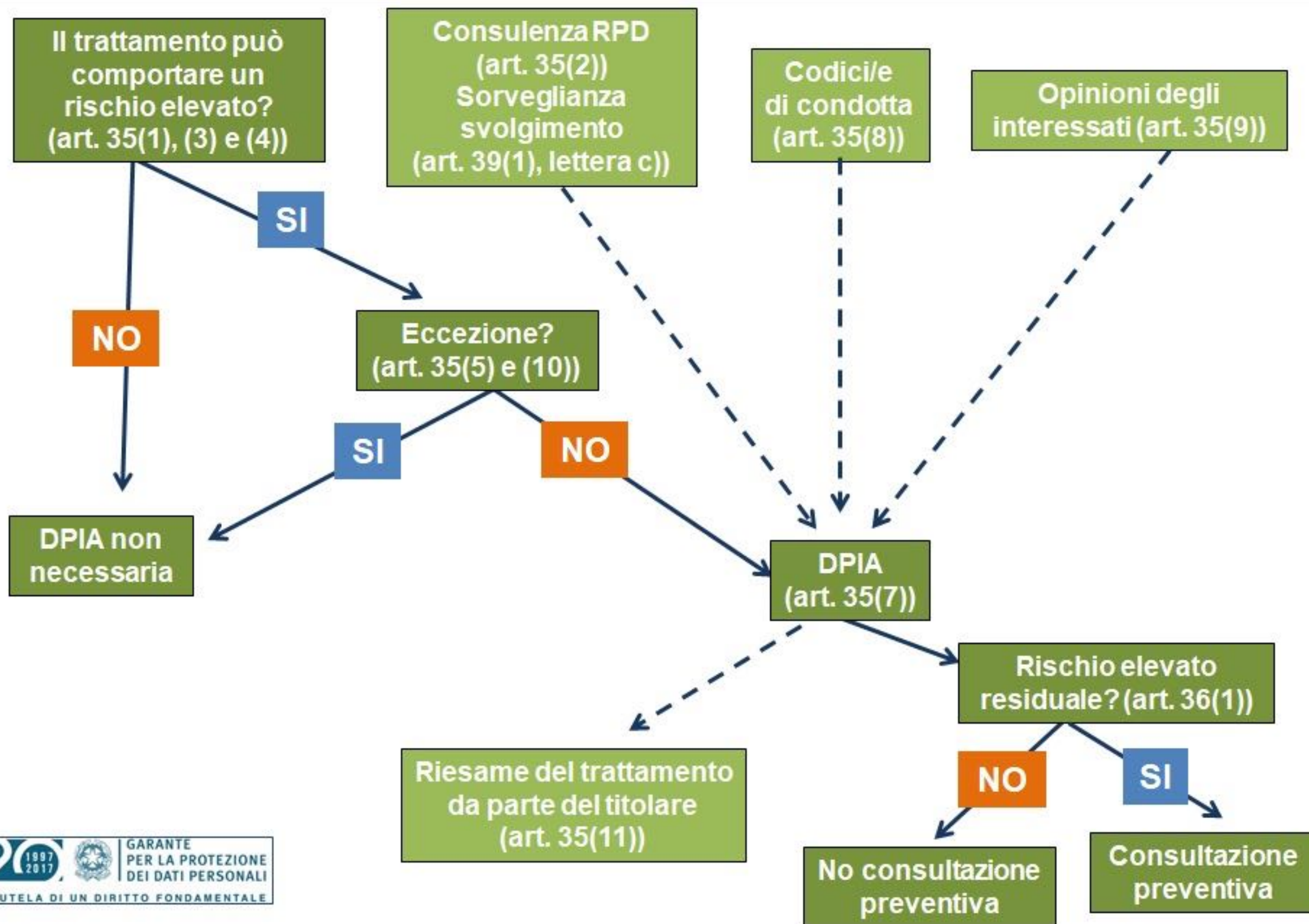
Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto

- 1. **Trattamenti valutativi o di scoring su larga scala**, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad “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. **Trattamenti automatizzati** finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi).
- 3. **Trattamenti che prevedono un utilizzo sistematico di dati** per l’osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell’informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d’uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

- **4. Trattamenti su larga scala** di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
- **5. Trattamenti effettuati nell'ambito del rapporto di lavoro** mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
- **6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili** (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

- **7. Trattamenti effettuati attraverso l'uso di tecnologie innovative**, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualevolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .
- **8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.**
- **9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni**, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment)
- **10. Trattamenti di categorie particolari di dati** ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
- **11. Trattamenti sistematici di dati biometrici**, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
- **12. Trattamenti sistematici di dati genetici**, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

Valutazione di impatto sulla protezione dei dati (DPIA). Quando effettuarla?



Articolo 35

Valutazione d'impatto sulla protezione dei dati

1. 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**, 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.

Uso di nuove tecnologie

Natura, oggetto, contesto e finalità

Rischio per i diritti e le libertà delle persone fisiche

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.



Valutazione d'impatto sulla protezione dei dati

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 **è richiesta** in particolare nei casi seguenti:

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;



Profilazione

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; o



**categorie
particolari**

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



**sorveglianza
sistematica**

Valutazione d'impatto sulla protezione dei dati

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.
5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.
6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

Valutazione d'impatto sulla protezione dei dati

7. La valutazione contiene almeno:

- 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.

Valutazione d'impatto sulla protezione dei dati

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.
9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

Valutazione d'impatto sulla protezione dei dati

10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Articolo 6

Liceità del trattamento

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

- a) l'interessato ha espresso il **consenso al trattamento** dei propri dati personali per una o più specifiche finalità;
- b) il trattamento è **necessario all'esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- c) il trattamento è necessario per **adempiere un obbligo legale** al quale è soggetto il titolare del trattamento;
- d) il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;
- e) il trattamento è necessario per l'**esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento;
- f) il trattamento è necessario per il **perseguimento del legittimo interesse del titolare** del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI



17/IT

WP 248 rev.01

**Linee guida in materia di valutazione d'impatto sulla protezione dei dati e
determinazione della possibilità che il trattamento "possa presentare un rischio elevato"
ai fini del regolamento (UE) 2016/679**

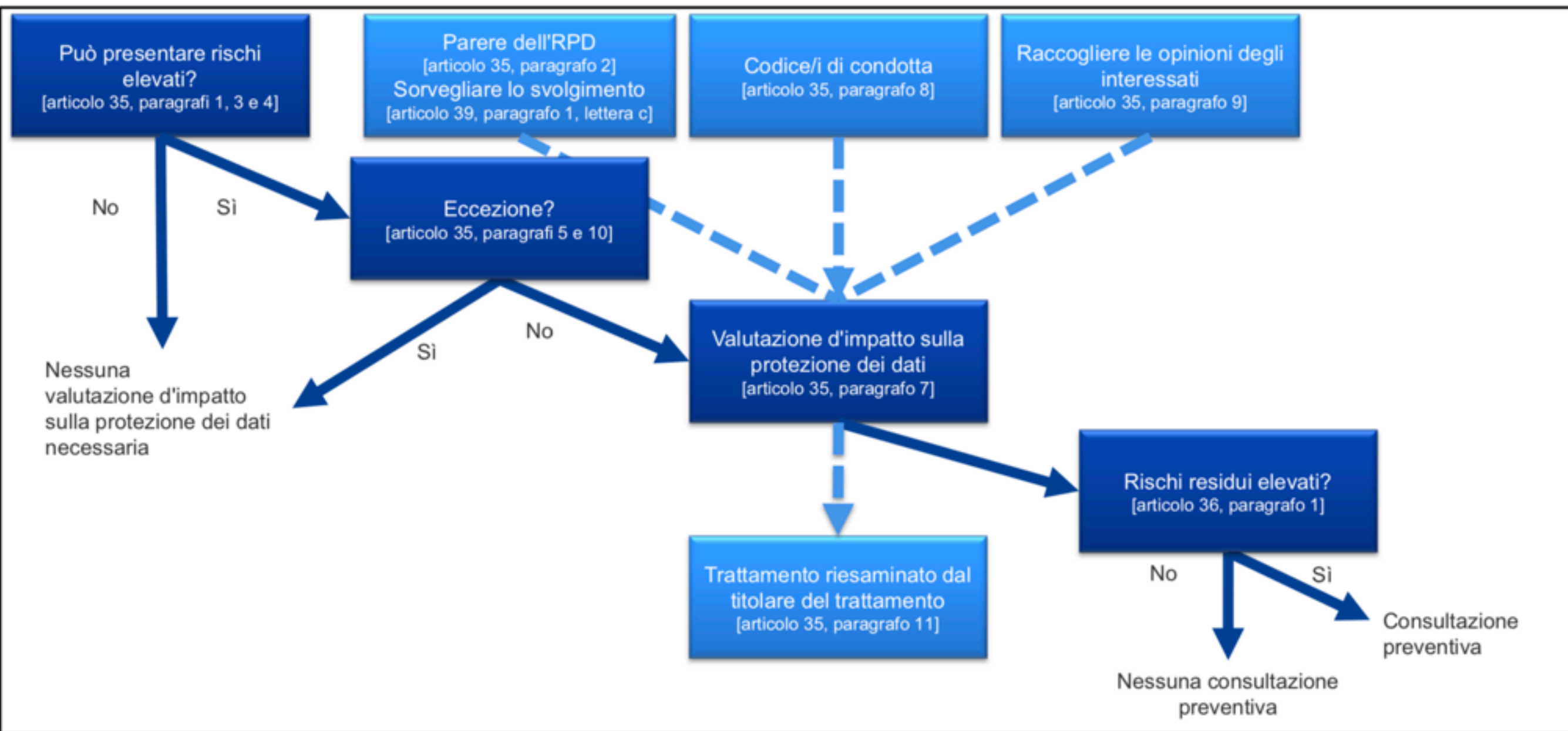
adottate il 4 aprile 2017

come modificate e adottate da ultimo il 4 ottobre 2017

Una valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento. In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, **non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento**. Infatti, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando il trattamento "**può presentare un rischio elevato per i diritti e le libertà delle persone fisiche**" (articolo 35, paragrafo 1).

Al fine di assicurare un'interpretazione coerente delle circostanze in cui è obbligatorio realizzare una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 3), le presenti linee guida mirano innanzitutto a chiarire tale nozione e a fornire criteri per gli elenchi che devono essere adottati dalle autorità di protezione dei dati ai sensi dell'articolo 35, paragrafo 4.



insieme dei trattamenti che richiedono una valutazione d'impatto sulla protezione dei dati in virtù del loro rischio elevato intrinseco, tenendo conto degli elementi particolari di cui all'articolo 35, paragrafo 1 e all'articolo 35, paragrafo 3, lettere da a) a c), l'elenco da adottare a livello nazionale ai sensi dell'articolo 35, paragrafo 4, e dei considerando 71, 75 e 91, e di altri riferimenti del regolamento generale sulla protezione dei dati a trattamenti che "possono presentare un rischio elevato"¹⁴, si devono considerare i seguenti **nove criteri**.

1. **Valutazione** o assegnazione di un **punteggio**, **inclusiva di profilazione e previsione**

Valutazione o assegnazione di un punteggio, inclusiva di **profilazione** e **previsione**, in particolare in considerazione 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**" (considerando 71 e 91). Esempi di ciò potrebbero includere: un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso;

2. processo decisionale automatizzato che ha **effetto giuridico**

processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: **trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche"** (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico. Ulteriori spiegazioni in merito a queste nozioni saranno fornite nelle linee guida sulla profilazione che saranno pubblicate prossimamente dal WP29;

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))¹⁵. Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);

4. dati sensibili o dati aventi carattere altamente personale

questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle **opinioni politiche** delle persone), nonché dati personali relativi a **condanne penali o reati** di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le **comunicazioni elettroniche** la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i **dati relativi all'ubicazione**, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a **dati finanziari** che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali **documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone;**

5. trattamento di dati su larga scala

il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala¹⁶:

- il **numero di soggetti interessati dal trattamento**, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il **volume dei dati e/o le diverse tipologie di dati** oggetto di trattamento;
- la **durata, ovvero la persistenza**, dell'attività di trattamento;
- la **portata geografica** dell'attività di trattamento;

6. creazione di corrispondenze o combinazione di insiemi di dati

creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato

7. dati relativi a interessati vulnerabili

(considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono **non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti**. Gli interessati vulnerabili possono includere i **minori** (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i **dipendenti**, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (**infermi di mente, richiedenti asilo o anziani, pazienti**, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;

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

uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'**impronta digitale** e del **riconoscimento facciale** per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi. Ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una valutazione d'impatto sulla protezione dei dati;

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). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto. Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno.

Nella maggior parte dei casi, un titolare del trattamento può considerare che un trattamento che soddisfi **due criteri** debba formare oggetto di una valutazione d'impatto sulla protezione dei dati. In generale, 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 e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati, indipendentemente dalle misure che il titolare del trattamento ha previsto di adottare.

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 sulla protezione dei dati, nonché includere/registrazione i punti di vista del responsabile della protezione dei dati.

Il WP29 ritiene che una valutazione d'impatto sulla protezione dei dati non sia richiesta nei seguenti casi:

- quando il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1);
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo (articolo 35, paragrafo 119);
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate²⁰ (cfr. III.C);
- qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10)²¹, a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;
- qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5). Tale elenco può contenere attività di trattamento conformi alle condizioni specificate da detta autorità, in particolare attraverso linee guida, decisioni o autorizzazioni specifiche, norme di conformità, ecc. (ad esempio in Francia, autorizzazioni, esenzioni, norme semplificate, pacchetti di conformità, ecc.). In tali casi e a condizione che venga eseguita una nuova valutazione da parte dell'autorità di controllo competente, non è richiesta una valutazione d'impatto sulla protezione dei dati, ma soltanto se il trattamento rientra a tutti gli effetti nel campo di applicazione della procedura pertinente menzionata nell'elenco e continua a rispettare pienamente tutti i requisiti pertinenti del regolamento generale sulla protezione dei dati.

C. Quale regola si applica ai trattamenti già esistenti? In talune circostanze sono richieste valutazioni d'impatto sulla protezione dei dati.

L'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati 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.

[...]

Secondo le buone prassi, una valutazione d'impatto sulla protezione dei dati va riesaminata continuamente e rivalutata con regolarità. Di conseguenza, anche se una valutazione d'impatto sulla protezione dei dati non è richiesta il 25 maggio 2018, al momento opportuno, il titolare del trattamento sarà tenuto a svolgere tale valutazione nel contesto dei suoi obblighi generali di responsabilizzazione.

D. Come va svolta una valutazione d'impatto sulla protezione dei dati?

La valutazione d'impatto sulla protezione dei dati 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.

La valutazione d'impatto sulla protezione dei dati va avviata il prima possibile nella fase di progettazione del trattamento anche se alcune delle operazioni di trattamento non sono ancora note. L'aggiornamento della valutazione d'impatto sulla protezione dei dati nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità. Può essere altresì necessario ripetere singole fasi della valutazione man mano che il processo di sviluppo evolve, dato che la selezione di determinate misure tecniche od organizzative può influenzare la gravità o la probabilità dei rischi posti dal trattamento.

Il fatto che possa rendersi necessario aggiornare la valutazione d'impatto sulla protezione dei dati dopo l'effettivo avvio del trattamento non costituisce un motivo valido per rinviare o non svolgere una valutazione d'impatto sulla protezione dei dati. La valutazione d'impatto sulla protezione dei dati è un processo continuo, soprattutto quando un trattamento è dinamico ed è soggetto a variazioni continue.

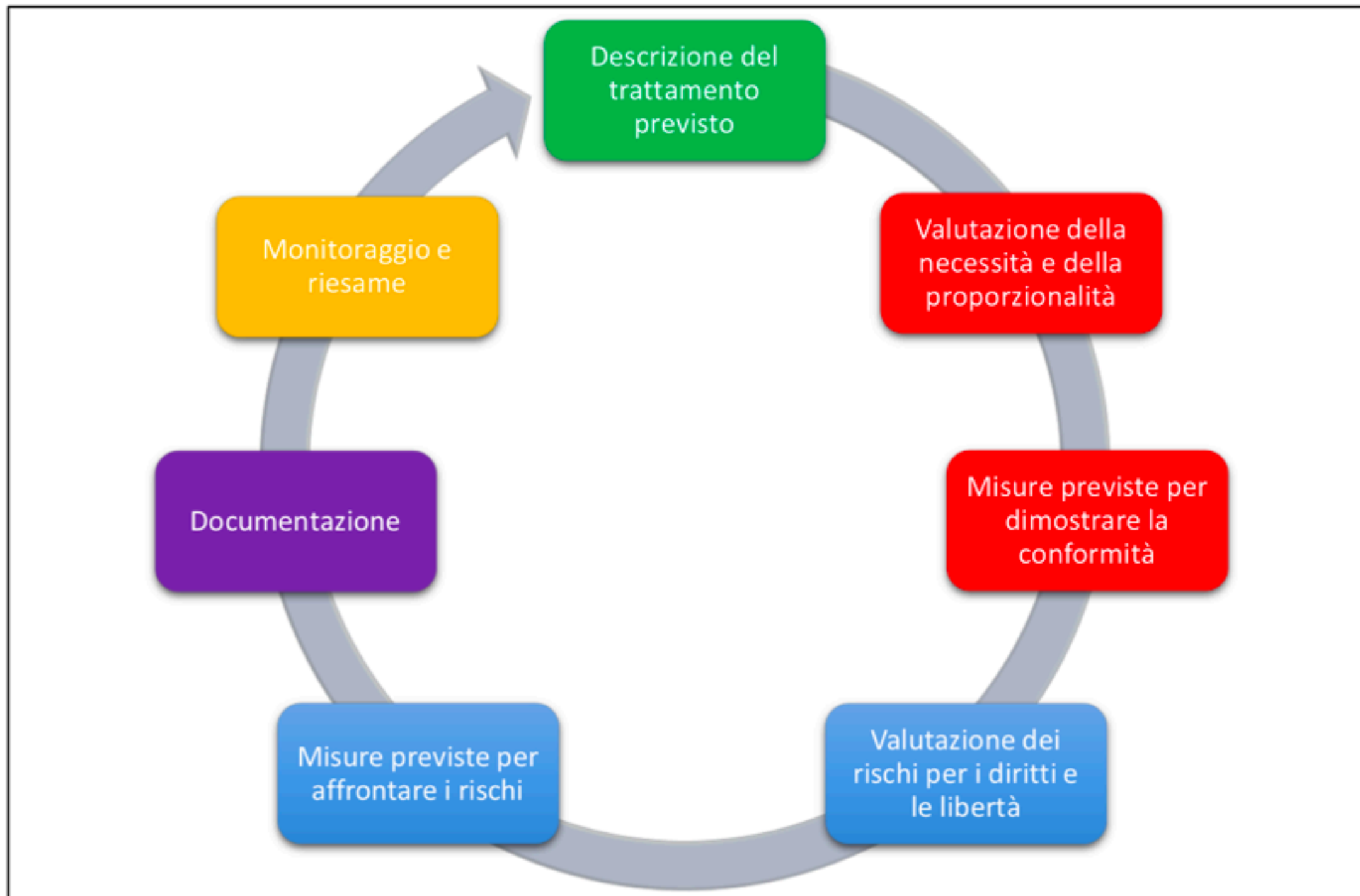
Realizzare una
valutazione d'impatto
sulla protezione dei dati è
un processo continuo,
non un esercizio una
tantum.

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.

Inoltre 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)). Ulteriori orientamenti in merito sono forniti nelle "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 - 16/EN WP 243.

Qualora il trattamento venga eseguito in toto o in parte da un responsabile del trattamento dei dati, quest'ultimo deve assistere il titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati e fornire tutte le informazioni necessarie (conformemente all'articolo 28, paragrafo 3, lettera f)).

processo iterativo generico per lo svolgimento di una valutazione d'impatto sulla protezione dei dati



La pubblicazione di una valutazione d'impatto sulla protezione dei dati non è un requisito giuridico sancito dal regolamento generale sulla protezione dei dati, è una decisione del titolare del trattamento procedere in tal senso. Tuttavia, i titolari del trattamento dovrebbero prendere in considerazione la pubblicazione di almeno alcune parti, ad esempio di una sintesi o della conclusione della loro valutazione d'impatto sulla protezione dei dati.

Ogniqualevolta il titolare del trattamento 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.

Articolo 36

Consultazione preventiva

1. Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un **rischio elevato** in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.
2. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.