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

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI,

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 della stessa,

visto il suo regolamento interno,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Indice

I. Introduzione

Il regolamento (UE) 2016/679[1] ("regolamento generale sulla protezione dei dati") si applicherà a partire dal 25 maggio 2018. L'articolo 35 del regolamento generale sulla protezione dei dati introduce il concetto di valutazione d'impatto sulla protezione dei dati[2], così come previsto anche dalla direttiva 2016/680[3].

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[4], 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 (cfr. anche l'articolo 24)[5]. In altre parole, **una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità**.

A norma del regolamento generale sulla protezione dei dati, l'inosservanza dei requisiti stabiliti per la valutazione d'impatto sulla protezione dei dati può portare a sanzioni pecuniarie imposte dall'autorità

---

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[2] In altri contesti il termine "valutazione dell'impatto sulla vita privata" è spesso utilizzato per fare riferimento allo stesso concetto.

[3] L'articolo 27 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, prevede altresì che sia necessaria una valutazione dell'impatto sulla vita privata "*quando il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*".

[4] Il regolamento generale sulla protezione dei dati non definisce formalmente il concetto di valutazione d'impatto sulla protezione dei dati come tale, tuttavia

- il suo contenuto minimo è specificato dall'articolo 35, paragrafo 7, come segue:
  - *"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";*
- il suo significato e il suo ruolo sono chiariti dal considerando 84 come segue: *"[p]er potenziare il rispetto del presente regolamento 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"*.

[5] Cfr. anche il considerando 84: *"[l]'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento"*.

di controllo competente. La mancata esecuzione di una valutazione d'impatto sulla protezione dei dati nei casi in cui il trattamento è soggetto alla stessa (articolo 35, paragrafi 1, 3 e 4), l'esecuzione in maniera errata di detta valutazione (articolo 35, paragrafi 2 e da 7 a 9) oppure la mancata consultazione dell'autorità di controllo laddove richiesto (articolo 36, paragrafo 3, lettera e)), possono comportare una sanzione amministrativa pecuniaria pari a un importo massimo di 10 milioni di EUR oppure, nel caso di un'impresa, pari a fino al 2% del fatturato annuo globale dell'anno precedente, a seconda di quale dei due importi sia quello superiore.

II. Campo di applicazione delle presenti linee guida

Le presenti linee guida tengono conto dei seguenti documenti:

- dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN WP 218[6];
- linee guida sui responsabili della protezione dei dati del WP29 - 16/EN WP 243[7];
- parere del WP29 sulla limitazione della finalità - 13/EN WP 203[8];
- norme internazionali[9].

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.

A norma dell'articolo 70, paragrafo 1, lettera e), il comitato europeo per la protezione dei dati potrà pubblicare linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del regolamento generale sulla protezione dei dati. Lo scopo del presente documento è quindi quello di anticipare i futuri lavori del comitato europeo per la protezione dei dati e, di conseguenza, di chiarire le pertinenti disposizioni del regolamento generale sulla protezione dei dati in maniera da

---

[6] "*WP29 Statement 14/EN WP 218 on the role of a risk-based approach to data protection legal frameworks*" [Dichiarazione del WP29 14/EN WP 218 sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati], adottata il 30 maggio 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532.

[7] documento 16/EN WP 243 "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 adottate il 13 dicembre 2016.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A.

[8] "*WP29 Opinion 03/2013 on purpose limitation*" [Parere 03/2013 del WP29 sulla limitazione della finalità] - 13/EN WP 203, approvato il 2 aprile 2013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409.

[9] Ad esempio la norma ISO 31000:2009, *Gestione del rischio - Principi e linee guida*, Organizzazione internazionale per la normazione (ISO); ISO/IEC 29134 (progetto), *Information technology – Security techniques – Privacy impact assessment – Guidelines* (in inglese), Organizzazione internazionale per la normazione (ISO).

assistere i titolari del trattamento nel rispettare la legge, nonché da fornire la certezza del diritto a quei titolari del trattamento che sono tenuti a realizzare una valutazione d'impatto sulla protezione dei dati.

Le presenti linee guida mirano altresì a promuovere la redazione di:

- un elenco comune dell'Unione europea delle tipologie di trattamento per le quali è obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 4);
- un elenco comune dell'Unione europea delle tipologie di trattamento per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5);
- criteri comuni sulla metodologia per la realizzazione di una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5);
- criteri comuni che specifichino quando è necessario consultare l'autorità di controllo (articolo 36, paragrafo 1);
- raccomandazioni, ove possibile, basate sull'esperienza acquisita negli Stati membri dell'UE.

III. Valutazione d'impatto sulla protezione dei dati: spiegazione del regolamento

Il regolamento generale sulla protezione dei dati prevede che i titolari del trattamento attuino misure adeguate per garantire ed essere in grado di dimostrare il rispetto di detto regolamento, tenendo conto tra l'altro dei "rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (articolo 24, paragrafo 1) . L'obbligo per i titolari del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati va inteso nel contesto dell'obbligo generale, cui gli stessi sono soggetti, di gestire adeguatamente i rischi[10] presentati dal trattamento di dati personali.

Un "rischio" è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. La "gestione dei rischi", invece, può essere definita come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

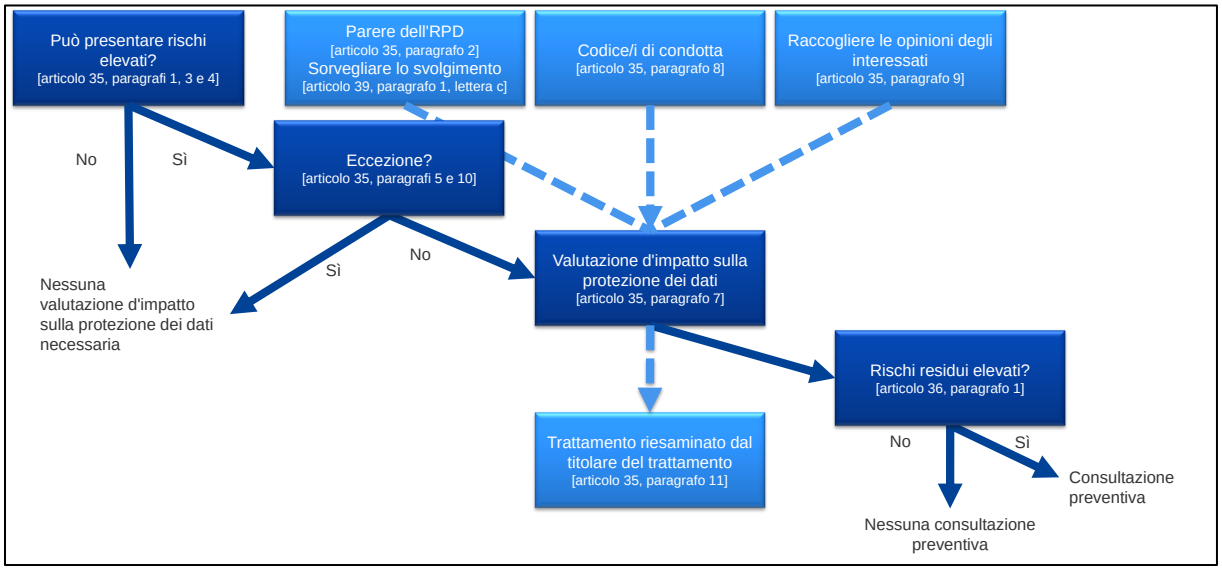
L'articolo 35 fa riferimento al possibile rischio elevato "per i diritti e le libertà delle persone fisiche". Come indicato nella dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati, 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.

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. Al contrario, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1). Il semplice fatto che le condizioni che comportano l'obbligo di realizzare una valutazione d'impatto sulla protezione dei dati non siano soddisfatte non diminuisce tuttavia l'obbligo generale, cui i titolari del trattamento sono soggetti, di attuare misure volte a gestire adeguatamente i rischi per i diritti e le libertà degli interessati. In pratica, ciò significa

[10] Va sottolineato che al fine di poter gestire i rischi per i diritti e le libertà delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. I titolari del trattamento non possono sottrarsi alla loro responsabilità coprendo i rischi stipulando polizze assicurative.

che i titolari del trattamento devono continuamente valutare i rischi creati dalle loro attività al fine di stabilire quando una tipologia di trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche".

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:



A. Che cosa esamina una valutazione d'impatto sulla protezione dei dati? Un singolo trattamento o un insieme di trattamenti simili.

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*". Il considerando 92 aggiunge che "*[v]i sono circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata*".

Si potrebbe 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. In effetti, le valutazioni d'impatto sulla protezione dei dati mirano a studiare sistematicamente nuove situazioni che potrebbero portare a rischi elevati per i diritti e le libertà delle persone fisiche e non è necessario realizzare una valutazione d'impatto sulla protezione dei dati nei casi (ad esempio operazioni di trattamento in un contesto specifico e per una finalità specifica) che sono già stati studiati. Questo potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità. Ad esempio, un gruppo di autorità comunali che istituiscono ciascuna un sistema di televisione a circuito chiuso simile potrebbe svolgere una singola valutazione d'impatto sulla protezione dei dati che copra il trattamento svolto da tali titolari del trattamento distinti; oppure un gestore ferroviario (un titolare del trattamento unico) potrebbe esaminare la videosorveglianza in tutte le sue stazioni ferroviarie realizzando una singola valutazione d'impatto sulla protezione dei dati. Ciò può essere applicabile anche a trattamenti simili attuati da vari titolari del

trattamento di dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile una valutazione d'impatto sulla protezione dei dati di riferimento, attuare le misure descritte nella stessa, e fornire una giustificazione per la realizzazione di una singola valutazione d'impatto sulla protezione dei dati.

Qualora il trattamento coinvolga contitolari del trattamento, questi ultimi devono definire con precisione le rispettive competenze. La loro valutazione d'impatto sulla protezione dei dati deve stabilire quale parte sia competente per le varie misure volte a trattare i rischi e a proteggere i diritti e le libertà degli interessati. Ciascun titolare del trattamento deve esprimere le proprie esigenze e condividere informazioni utili senza compromettere eventuali segreti (ad esempio protezione di segreti aziendali, proprietà intellettuale, informazioni aziendali riservate) o divulgare vulnerabilità.

Una valutazione d'impatto sulla protezione dei dati può essere altresì utile per valutare l'impatto sulla protezione dei dati di un prodotto tecnologico, ad esempio un dispositivo hardware o un software, qualora sia probabile che lo stesso venga utilizzato da titolari del trattamento distinti per svolgere tipologie diverse di trattamento. Ovviamente, il titolare del trattamento che utilizza detto prodotto resta soggetto all'obbligo di svolgere la propria valutazione d'impatto sulla protezione dei dati in relazione all'attuazione specifica, tuttavia tale valutazione del titolare del trattamento può utilizzare le informazioni fornite da una valutazione analoga preparata dal fornitore del prodotto, se opportuno. Un esempio potrebbe essere rappresentato dalla relazione tra produttori di contatori intelligenti e società fornitrici di servizi pubblici. Ogni fornitore di prodotti o responsabile del trattamento dovrebbe condividere informazioni utili senza compromettere i segreti né generare rischi per la sicurezza, divulgando vulnerabilità.

B. Quali trattamenti sono soggetti a una valutazione d'impatto sulla protezione dei dati? Escludendo le eccezioni, in tutti i casi in cui tali trattamenti "*possono presentare un rischio elevato*".

Questa sezione descrive i casi nei quali è richiesta una valutazione d'impatto sulla protezione dei dati e quelli che invece non la richiedono.

Fatti salvi i casi in cui un trattamento rientra nel campo di applicazione di un'eccezione (III.B.a), è necessario realizzare una valutazione d'impatto sulla protezione dei dati qualora un trattamento "*possa presentare un rischio elevato***" (III.B.b).**

a) Quando è obbligatoria una valutazione d'impatto sulla protezione dei dati? Quando il trattamento "*può presentare un rischio elevato*".

Il regolamento generale sulla protezione dei dati non richiede la realizzazione di una valutazione d'impatto sulla protezione dei dati per ciascun trattamento che può presentare rischi per i diritti e le libertà delle persone fisiche. La realizzazione di una valutazione d'impatto sulla protezione dei dati è obbligatoria soltanto qualora il trattamento "*possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (articolo 35, paragrafo 1, illustrato dall'articolo 35, paragrafo 3, e integrato dall'articolo 35, paragrafo 4). Essa è particolarmente importante quando viene introdotta una nuova tecnologia di trattamento dei dati[11].

[11] Cfr. i considerando 89 e 91 e l'articolo 35, paragrafi 1 e 3, per ulteriori esempi.

Nei casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, il WP29 raccomanda di effettuarla comunque, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati.

Sebbene una valutazione d'impatto sulla protezione dei dati possa essere richiesta anche in altre circostanze, 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 fisiche*[12]*;*
- *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*[13]*; o*
- *c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".*

Come indicato dalle parole "*in particolare*" nella frase introduttiva dell'articolo 35, paragrafo 3, del regolamento generale sulla protezione dei dati, questo va inteso come un elenco non esaustivo. Vi possono essere operazioni di trattamento a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto elevati. Anche tali trattamenti devono essere soggetti alla realizzazione di valutazioni d'impatto sulla protezione dei dati. Per questo motivo, i criteri sviluppati qui di seguito vanno, talvolta, al di là di una semplice spiegazione dell'interpretazione dei tre esempi di cui all'articolo 35, paragrafo 3, del regolamento generale sulla protezione dei dati.

Al fine di fornire un insieme più concreto di 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, 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;

---

[12] Cfr. considerando 71: *"in particolare mediante l'analisi o la previsione 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, al fine di creare o utilizzare profili personali".*

[13] Cfr. considerando 75: *"se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza"* .

[14] Cfr. ad esempio i considerando 75, 76, 92 e 116.

2. 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;

---

[15] L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del WP29 (cfr. le "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 - 16/EN WP 243):

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Il termine "*zona accessibile al pubblico*", a giudizio del WP29, indica qualsiasi luogo aperto a ciascun individuo della popolazione, come ad esempio una piazza, un centro commerciale, una strada, un mercato, una stazione ferroviaria o una biblioteca pubblica.

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 scala[16]:
    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;
6. 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[17];
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, 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.

[16] Cfr. "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 - 16/EN WP 243.
[17] Cfr. spiegazione contenuta nel parere del WP29 sulla limitazione della finalità - 13/EN WP 203, pag. 24.

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.

Tuttavia, 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.**

Gli esempi riportati di seguito illustrano come utilizzare i criteri per valutare se una particolare tipologia di trattamento richieda una valutazione d'impatto sulla protezione dei dati o meno.

Esempi di trattamento	**Possibili criteri pertinenti**	**È probabile che sia richiesta una valutazione d'impatto sulla protezione dei dati?**
Un ospedale che tratta i dati genetici e sanitari dei propri pazienti (sistema informativo ospedaliero).	- Dati sensibili o dati aventi carattere estremamente personale. - Dati riguardanti soggetti interessati vulnerabili. - Trattamento di dati su larga scala.	Sì
L'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade. Il titolare del trattamento prevede di utilizzare un sistema intelligente di analisi video per individuare le auto e riconoscere automaticamente le targhe.	- Monitoraggio sistematico. - Uso innovativo o applicazione di soluzioni tecnologiche od organizzative.	
Un'azienda che monitora sistematicamente le attività dei suoi dipendenti, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, ecc.	- Monitoraggio sistematico. - Dati riguardanti soggetti interessati vulnerabili.	
La raccolta di dati pubblici dei media sociali per la generazione di profili.	- Valutazione o assegnazione di un punteggio. - Trattamento di dati su larga scala. - Creazione di corrispondenze o combinazione di insiemi di dati. - Dati sensibili o dati aventi carattere estremamente personale.	

Esempi di trattamento	Possibili criteri pertinenti	È probabile che sia richiesta una valutazione d'impatto sulla protezione dei dati?
Un'istituzione che crea una banca dati antifrode e di gestione del rating del credito a livello nazionale.	- Valutazione o assegnazione di un punteggio. - Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente. - Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto. - Dati sensibili o dati aventi carattere estremamente personale.	
Conservazione per finalità di archiviazione di dati sensibili personali pseudonimizzati relativi a interessati vulnerabili coinvolti in progetti di ricerca o sperimentazioni cliniche.	- Dati sensibili. - Dati riguardanti soggetti interessati vulnerabili. - Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto.	
Un trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" (considerando 91).	- Dati sensibili o dati aventi carattere estremamente personale. - Dati riguardanti soggetti interessati vulnerabili.	No
Una rivista online che utilizza una lista di distribuzione per inviare una selezione quotidiana generica ai suoi abbonati.	- Trattamento di dati su larga scala.	
Un sito web di commercio elettronico che visualizza annunci pubblicitari per parti di auto d'epoca che comporta una limitata profilazione basata sugli articoli visualizzati o acquistati sul proprio sito web.	- Valutazione o assegnazione di un punteggio.	

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/registrare i punti di vista del responsabile della protezione dei dati.

Inoltre, nel contesto del principio di responsabilizzazione, ogni titolare del trattamento deve tenere "*un registro delle attività di trattamento svolte sotto la propria responsabilità*" che includa, tra l'altro, le finalità del trattamento, una descrizione delle categorie di dati e di destinatari dei dati e "*ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1*" (articolo 30, paragrafo 1); inoltre, deve valutare la probabilità di un rischio elevato, anche qualora decida in ultima analisi di non realizzare una valutazione d'impatto sulla protezione dei dati.

Nota: le autorità di controllo sono tenute a stabilire, rendere pubblico e comunicare al comitato europeo per la protezione dei dati un elenco delle tipologie di trattamento che richiedono una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 4)[18]. I criteri di cui sopra possono aiutare le autorità di controllo a redigere un tale elenco, aggiungendo contenuti specifici nel corso del tempo, se applicabile. Ad esempio, anche il trattamento di qualsiasi tipo di dati biometrici o di dati di minori potrebbe essere considerato pertinente per lo sviluppo di un elenco ai sensi dell'articolo 35, paragrafo 4.

b) Quando non è richiesta una valutazione d'impatto sulla protezione dei dati? Quando il trattamento non è tale da "*presentare un rischio elevato*" oppure qualora esista una valutazione d'impatto sulla protezione dei dati analoga, o qualora il trattamento sia stato autorizzato prima del maggio 2018 oppure abbia una base giuridica o sia incluso nell'elenco delle tipologie di trattamento per le quali non è richiesta una valutazione d'impatto sulla 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 1[19]);
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate[20] (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

[18] In tale contesto, "*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*" (articolo 35, paragrafo 6).

[19] "*Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*".

[20] "*Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate*" (considerando 171).

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.

Non è necessaria una valutazione d'impatto sulla protezione dei dati per i trattamenti che sono stati verificati da un'autorità di controllo o dal responsabile della protezione dei dati, a norma dell'articolo 20 della direttiva 95/46/CE e che vengono eseguiti in maniera tale da fare sì che non si sia registrata alcuna variazione rispetto alla verifica precedente. In effetti, "*[l]e decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate*" (considerando 171).

Al contrario, ciò significa che qualsiasi trattamento di dati le cui condizioni di attuazione (ambito di applicazione, finalità, dati personali raccolti, identità dei titolari del trattamento o dei destinatari, periodo di conservazione dei dati, misure tecniche e organizzative, ecc.) sono mutate rispetto alla prima verifica effettuata dall'autorità di controllo o dal responsabile della protezione dei dati e che possono presentare un rischio elevato devono essere soggette a una valutazione d'impatto sulla protezione dei dati.

Inoltre, potrebbe essere richiesta una valutazione d'impatto sulla protezione dei dati in seguito a una variazione dei rischi derivante dalle operazioni di trattamento[22], ad esempio perché è entrata in uso una nuova tecnologia o perché i dati personali vengono utilizzati per una finalità diversa. Le operazioni di

[21] Quando viene svolta una valutazione d'impatto sulla protezione dei dati in fase di elaborazione della legislazione che fornisce una base giuridica per un trattamento, è probabile che la stessa richieda un riesame prima dell'avvio delle attività, in quanto la legislazione adottata può differire dalla proposta ed influenzare quindi questioni in materia di vita privata e protezione dei dati. Inoltre, potrebbero non esserci sufficienti dettagli tecnici per quanto riguarda il trattamento effettivo al momento dell'adozione della legislazione, anche qualora detto trattamento sia accompagnato da una valutazione d'impatto sulla protezione dei dati. In questi casi, può comunque essere necessario eseguire una valutazione d'impatto sulla protezione dei dati specifica prima di realizzare le attività di trattamento effettive.

[22] In termini di contesto, i dati raccolti, le finalità, le funzionalità, i dati personali trattati, i destinatari, le combinazioni di dati, i rischi (risorse di sostegno, fonti di rischio, impatti potenziali , minacce, ecc.), le misure di sicurezza e i trasferimenti internazionali.

trattamento dei dati possono evolversi rapidamente e potrebbero emergere nuove vulnerabilità. Di conseguenza, va osservato che la revisione di una valutazione d'impatto sulla protezione dei dati non è utile soltanto ai fini di un miglioramento continuo, bensì anche fondamentale per mantenere il livello di protezione dei dati in un ambiente che muta nel corso del tempo. Una valutazione d'impatto sulla protezione dei dati potrebbe rendersi necessaria anche perché il contesto organizzativo o sociale per l'attività di trattamento è mutato, ad esempio perché gli effetti di determinate decisioni automatizzate sono diventati più significativi oppure perché nuove categorie di interessati sono diventati vulnerabili alla discriminazione. Ciascuno di questi esempi potrebbe costituire un aspetto che porta a una variazione del rischio derivante dall'attività di trattamento interessata.

Al contrario, talune modifiche potrebbero anche ridurre il rischio. Ad esempio, un trattamento potrebbe evolvere in modo tale da fare sì che le decisioni non siano più automatizzate oppure si pensi al caso in cui un'attività di monitoraggio non viene più eseguita in maniera sistematica. In questo caso, il riesame dell'analisi dei rischi può mostrare che non è più necessario eseguire una valutazione d'impatto sulla protezione dei dati.

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?

a) In quale momento va effettuata una valutazione d'impatto sulla protezione dei dati? Prima del trattamento.

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.

[23] Fatto salvo il caso in cui si tratti di un trattamento già in essere che è stato preventivamente verificato dall'autorità di controllo, nel qual caso la valutazione d'impatto sulla protezione dei dati deve essere eseguita prima di attuare modifiche significative.

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

b) Chi è obbligato a effettuare la valutazione d'impatto sulla protezione dei dati? Il titolare del trattamento, con il responsabile della protezione dei dati e i responsabili del trattamento.

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)).

Il titolare del trattamento deve "*raccoglie[re] le opinioni degli interessati o dei loro rappresentanti*" (articolo 35, paragrafo 9), "***se del caso***". Il WP29 ritiene che:

- tali opinioni possono essere raccolte attraverso una varietà di mezzi, a seconda del contesto (ad esempio uno studio generico relativo alla finalità e ai mezzi del trattamento, una domanda posta ai rappresentanti del personale oppure indagini abituali inviate ai futuri clienti del titolare del trattamento), assicurando che il titolare del trattamento disponga di una base giuridica valida per il trattamento di qualsiasi dato personale interessato nel raccogliere dette opinioni; sebbene sia opportuno osservare che il consenso al trattamento non è ovviamente un modo per raccogliere le opinioni degli interessati;
- qualora la decisione finale del titolare del trattamento si discosti dalle opinioni degli interessati, le sue motivazioni a sostegno del procedere o meno vanno documentate;
- il titolare del trattamento deve altresì documentare la sua giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che ciò non sia appropriato, ad esempio qualora ciò comporterebbe la riservatezza dei piani economici dell'impresa o sarebbe sproporzionato o impraticabile.

Infine, è buona prassi definire e documentare altri ruoli e responsabilità specifici, a seconda delle politiche, dei processi e delle norme interni, ad esempio:

- qualora specifiche unità aziendali propongano di svolgere una valutazione d'impatto sulla protezione dei dati, tali unità dovrebbero poi fornire contributi alla valutazione d'impatto sulla protezione dei dati ed essere coinvolte nel processo di convalida di detta valutazione;

- se del caso, si raccomanda di consultare esperti indipendenti che esercitano professioni diverse[24] (avvocati, esperti informatici, esperti di sicurezza, sociologi, esperti di etica, ecc.).
- i ruoli e le responsabilità dei responsabili del trattamento devono essere definiti contrattualmente; e la valutazione d'impatto sulla protezione dei dati deve essere svolta con l'assistenza di un responsabile del trattamento, tenendo conto della natura del trattamento e delle informazioni a disposizione di detto responsabile del trattamento (articolo 28, paragrafo 3, lettera f));
- il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, così come il responsabile della protezione dei dati, potrebbero suggerire al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento e dovrebbero assistere le parti interessate in relazione alla metodologia, contribuire alla valutazione della qualità della valutazione dei rischi e del grado di accettabilità del rischio residuo, nonché allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
- il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione, dovrebbero fornire assistenza al titolare del trattamento, nonché potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza.

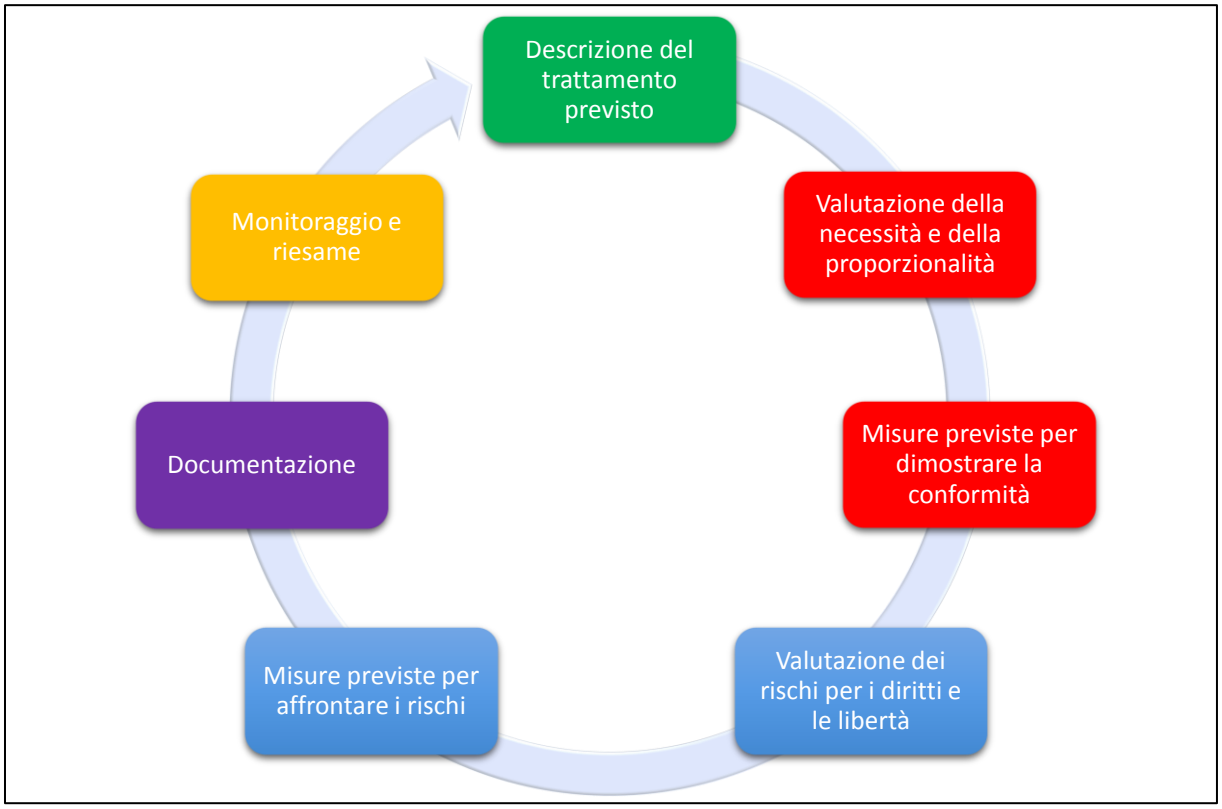
c) Qual è la metodologia da seguire per svolgere una valutazione d'impatto sulla protezione dei dati? Vi sono metodologie diverse, ma criteri comuni.

[24] *"Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3":* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

Il regolamento generale sulla protezione dei dati definisce le caratteristiche minime di una valutazione d'impatto sulla protezione dei dati (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:*
    - *"affrontare i rischi";*
    - *"dimostrare la conformità al presente regolamento".*

La figura che segue illustra il processo iterativo generico per lo svolgimento di una valutazione d'impatto sulla protezione dei dati[25]:



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 regolamento generale sulla protezione dei dati dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento (articolo 42), nonché rispetto alle norme vincolanti d'impresa.

[25] Va sottolineato che il processo descritto in questa sede è iterativo: in pratica, è probabile che ciascuna delle fasi venga riesaminata più volte prima che sia possibile completare la valutazione d'impatto sulla protezione dei dati.

Tutti i requisiti pertinenti stabiliti nel regolamento generale sulla protezione dei dati offrono un quadro ampio e generico per la progettazione e lo svolgimento di una valutazione d'impatto sulla protezione dei dati. L'attuazione pratica di una valutazione d'impatto sulla protezione dei dati dipenderà dai requisiti stabiliti nel regolamento generale sulla protezione dei dati che possono essere integrati da orientamenti pratici più dettagliati. L'attuazione della valutazione d'impatto sulla protezione dei dati è quindi modulabile. Ciò significa che anche un titolare del trattamento di piccole dimensioni può progettare e attuare una valutazione d'impatto sulla protezione dei dati adatta ai propri trattamenti.

Il considerando 90 del regolamento generale sulla protezione dei dati delinea una serie di elementi costituivi della valutazione d'impatto sulla protezione dei dati che si sovrappone a elementi ben definiti della gestione del rischio (ad esempio norma ISO 31000[26]). In termini di gestione dei rischi, una valutazione d'impatto sulla protezione dei dati mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche, utilizzando i seguenti processi:

- stabilendo il contesto: *"tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio";*
- valutando i rischi: *"valutare la particolare probabilità e gravità del rischio";*
- trattando i rischi: *"atten[uando] tale rischio*" e "*assicurando la protezione dei dati personali*", e "*dimostrando la conformità al presente regolamento*".

Nota: la valutazione d'impatto sulla protezione dei dati svolta ai sensi del regolamento generale sulla protezione dei dati è uno strumento per gestire i rischi per i diritti degli interessati, di conseguenza, adotta la loro prospettiva, come avviene in taluni settori (ad esempio, la sicurezza sociale). Al contrario, la gestione del rischio in altri settori (ad esempio in quello della sicurezza delle informazioni) è incentrata sull'organizzazione.

Il regolamento generale sulla protezione dei dati offre ai titolari del trattamento la flessibilità di stabilire la struttura e la forma precise della valutazione d'impatto sulla protezione dei dati in maniera da consentire che la stessa si adatti alle pratiche di lavoro esistenti. Esistono diversi processi stabiliti all'interno dell'UE e nel mondo che tengono conto degli elementi costitutivi descritti nel considerando 90. Tuttavia, indipendentemente dalla sua forma, una valutazione d'impatto sulla protezione dei dati deve essere una vera e propria valutazione dei rischi che consenta ai titolari del trattamento di adottare misure per affrontarli.

Si potrebbe ricorrere a metodologie diverse (cfr. allegato 1 per esempi di metodologie di valutazione dell'impatto sulla vita privata e sulla protezione dei dati) per contribuire all'attuazione dei requisiti essenziali stabiliti nel regolamento generale sulla protezione dei dati. Al fine di consentire l'esistenza di tali approcci distinti, permettendo comunque ai titolari del trattamento di rispettare il regolamento generale sulla protezione dei dati, sono stati individuati dei criteri comuni (cfr. allegato 2). Tali criteri chiariscono i requisiti essenziali del regolamento, ma offrono un campo di applicazione sufficiente da consentire la coesistenza di forme diverse di attuazione. Detti criteri possono essere utilizzati per dimostrare che una particolare metodologia di valutazione d'impatto sulla protezione dei dati soddisfa i parametri imposti dal regolamento generale sulla protezione dei dati. **Spetta al titolare del trattamento scegliere una metodologia che, comunque, deve essere conforme ai criteri di cui all'allegato 2.**

[26] Processi di gestione del rischio: comunicazione e consultazione, definizione del contesto, valutazione dei rischi, trattamento dei rischi, monitoraggio e riesame (cfr. termini e definizioni e l'indice nell'anteprima della norma ISO 31000 (in inglese): https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

Il WP29 incoraggia lo sviluppo di quadri di valutazione d'impatto sulla protezione dei dati specifici dei vari settori. Ciò è dovuto al fatto che essi possono attingere a conoscenze specifiche settoriali, aspetto questo che fa sì che la valutazione d'impatto sulla protezione dei dati possa affrontare le specificità di un particolare tipo di trattamento (ad esempio tipi particolari di dati, risorse aziendali, impatti potenziali, minacce, misure). Ciò significa che la valutazione d'impatto sulla protezione dei dati può affrontare le problematiche che sorgono in un settore economico specifico oppure quando si utilizzano tecnologie particolari o si eseguono tipologie particolari di trattamento.

Infine, 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 35, paragrafo 11[27]).

d) Esiste l'obbligo di pubblicare la valutazione d'impatto sulla protezione dei dati? No, tuttavia pubblicarne una sintesi potrebbe favorire la fiducia e la valutazione d'impatto sulla protezione dei dati completa deve essere comunicata all'autorità di controllo in caso di consultazione preventiva o su richiesta da parte delle autorità competenti per la protezione dei dati personali.

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 titolari 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.

Lo scopo di un tale processo sarebbe quello di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati dal titolare del trattamento, nonché di dimostrare la responsabilizzazione e la trasparenza. Costituisce una prassi particolarmente buona pubblicare una valutazione d'impatto sulla protezione dei dati nel caso in cui individui della popolazione siano influenzati dal trattamento interessato. Nello specifico, ciò potrebbe essere il caso in cui un'autorità pubblica realizza una valutazione d'impatto sulla protezione dei dati.

La valutazione d'impatto sulla protezione dei dati pubblicata non deve necessariamente contenere l'intera valutazione, soprattutto qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza per il titolare del trattamento o divulgare segreti commerciali o informazioni commerciali sensibili. In queste circostanze, la versione pubblicata potrebbe consistere soltanto in una sintesi delle principali risultanze della valutazione d'impatto sulla protezione dei dati o addirittura soltanto in una dichiarazione nella quale si afferma che la valutazione d'impatto sulla protezione dei dati è stata condotta.

Inoltre, laddove una valutazione d'impatto sulla protezione dei dati riveli la presenza di rischi residui elevati, il titolare del trattamento sarà tenuto a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento (articolo 36, paragrafo 1). In tale contesto, la valutazione d'impatto sulla protezione dei dati deve essere fornita completa (articolo 36, paragrafo 3, lettera e)).

[27] L'articolo 35, paragrafo 10, esclude esplicitamente soltanto l'applicazione dell'articolo 35, paragrafi da 1 a 7.

L'autorità di controllo può fornire il proprio parere[28] e procurerà di non compromettere segreti commerciali né divulgare vulnerabilità di sicurezza, in conformità con i principi applicabili in ciascuno Stato membro in materia di accesso del pubblico a documenti ufficiali.

E. Quando è necessario consultare l'autorità di controllo? Quando i rischi residui sono elevati.

Come spiegato in precedenza:

- è necessario realizzare una valutazione d'impatto sulla protezione dei dati quando il trattamento "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (articolo 35, paragrafo 1; cfr. III.B.a). A titolo di esempio, il trattamento di dati sanitari su larga scala è considerato un trattamento tale da presentare un rischio elevato e richiede la realizzazione di una valutazione d'impatto sulla protezione dei dati;
- di conseguenza, spetta al titolare del trattamento valutare i rischi per i diritti e le libertà degli interessati e individuale le misure[29] 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; cfr. III.C.c). un esempio, in caso di conservazione di dati personali su computer portatili, potrebbe essere l'utilizzo di adeguate misure di sicurezza tecniche e organizzative (crittografia efficace completa del disco, gestione di chiavi robuste, opportuno controllo degli accessi, backup protetti, ecc.) oltre al ricorso a politiche esistenti (avviso, consenso, diritto di accesso, diritto di opposizione, ecc.).

Nell'esempio sopra riportato relativo ai computer portatili, qualora i rischi siano stati considerati sufficientemente attenuati dal titolare del trattamento e in seguito alla lettura dell'articolo 36, paragrafo 1 e dei considerando 84 e 94, il trattamento può procedere senza la consultazione dell'autorità di controllo. È nei casi in cui il titolare del trattamento non riesca a trattare in maniera sufficiente i rischi individuati (ossia i rischi residui rimangono elevati) che questi deve consultare l'autorità di controllo.

Un esempio di un rischio residuo elevato inaccettabile include casi in cui gli interessati possano subire conseguenze significative, o addirittura irreversibili, che non possono superare (ad esempio: accesso illegittimo a dati che comportano una minaccia per la vita degli interessati, un loro licenziamento, un rischio finanziario) e/o quando appare evidente che il rischio si verificherà (ad esempio: poiché non si è in grado di ridurre il numero di persone che accedono ai dati a causa delle loro modalità di condivisione, utilizzo o distribuzione o quando non si può porre rimedio a una vulnerabilità ben nota).

Ogniqualvolta 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 controllo[30].

---

[28] La formulazione di un parere scritto a favore del titolare del trattamento è necessaria soltanto quando l'autorità di controllo ritiene che il trattamento previsto non sia conforme al regolamento a norma dell'articolo 36, paragrafo 2.

[29] Tra le quali si annoverano la considerazione degli orientamenti esistenti formulati dal comitato europeo per la protezione dei dati e dalle autorità di controllo, nonché dello stato dell'arte e dei costi di attuazione, come previsto dall'articolo 35, paragrafo 1.

[30] Nota: "*la pseudonimizzazione e la cifratura dei dati personali*" (così come la minimizzazione dei dati, meccanismi di controllo, ecc.) non sono necessariamente misure appropriate. Sono soltanto esempi. Le misure adeguate dipendono dal contesto e dai rischi, aspetti specifici dei trattamenti effettuati.

Inoltre, il titolare del trattamento dovrà consultare l'autorità di vigilanza qualora il diritto dello Stato membro in questione prescriva che i titolari del trattamento consultino l'autorità di controllo e/o ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica (articolo 36, paragrafo 5).

Occorre tuttavia sottolineare che, indipendentemente dal fatto che la consultazione dell'autorità di controllo sia richiesta o meno in base al livello di rischio residuo, sussistono comunque gli obblighi di conservare una registrazione della valutazione d'impatto sulla protezione dei dati e di aggiornamento di detta valutazione al momento opportuno.

IV. Conclusioni e raccomandazioni

Le valutazioni d'impatto sulla protezione dei dati sono uno strumento utile di cui dispongono i titolari del trattamento per attuare sistemi di trattamento dei dati conformi al regolamento generale sulla protezione dei dati e possono essere obbligatorie per talune tipologie di trattamenti. Hanno natura modulabile e possono assumere forme diverse, tuttavia il regolamento generale sulla protezione dei dati stabilisce i requisiti essenziali di una valutazione d'impatto sulla protezione dei dati efficace. I titolari del trattamento dovrebbero considerare la realizzazione di una valutazione d'impatto sulla protezione dei dati come un'attività utile e positiva che contribuisce alla conformità giuridica.

L'articolo 24, paragrafo 1, definisce la responsabilità fondamentale del titolare del trattamento in termini di rispetto del regolamento generale sulla protezione dei dati: *"Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario".*

La valutazione d'impatto sulla protezione dei dati è un aspetto fondamentale del rispetto del regolamento laddove si preveda di svolgere o si stia svolgendo un trattamento di dati soggetto a rischio elevato. Ciò significa che i titolari del trattamento dovrebbero utilizzare i criteri stabiliti nel presente documento per stabilire se devono realizzare una valutazione d'impatto sulla protezione dei dati o meno. La politica interna dei titolari del trattamento potrebbe estendere questo elenco andando oltre i requisiti giuridici sanciti dal regolamento generale sulla protezione dei dati. Ciò dovrebbe suscitare un maggior senso di fiducia e riservatezza negli interessati e in altri titolari del trattamento.

Qualora si preveda di effettuare un trattamento che possa presentare un rischio elevato, il titolare del trattamento deve:

- scegliere una metodologia per la valutazione d'impatto sulla protezione dei dati (esempi riportati nell'allegato 1) che soddisfi i criteri di cui all'allegato 2, oppure specificare ed attuare un processo sistematico di valutazione d'impatto sulla protezione dei dati che:
    - sia conforme ai criteri di cui all'allegato 2;
    - sia integrata nei processi in materia di progettazione, sviluppo, cambiamento, rischio e riesame operativo in conformità con i processi, il contesto e la cultura interni;
    - coinvolga le parti interessate appropriate e definisca chiaramente le loro responsabilità (titolare del trattamento, responsabile della protezione dei dati, interessati o loro rappresentanti, imprese, servizi tecnici, responsabili del trattamento, responsabile della sicurezza dei sistemi d'informazione, ecc.);

- fornire la relazione relativa alla valutazione d'impatto sulla protezione dei dati all'autorità di controllo, laddove gli venga richiesto di procedere in tal senso;
- consultare l'autorità di controllo, qualora il titolare del trattamento non sia riuscito a determinare misure sufficienti per attenuare i rischi elevati;
- riesaminare periodicamente la valutazione d'impatto sulla protezione dei dati e il trattamento che essa valuta, almeno quando si registra una variazione del rischio posto dal trattamento;
- documentare le decisioni prese.

Allegato 1 - Esempi di quadri UE esistenti di valutazione d'impatto sulla protezione dei dati

Il regolamento generale sulla protezione dei dati non specifica quale processo di valutazione d'impatto sulla protezione dei dati debba essere seguito, ma consente piuttosto ai titolari del trattamento di introdurre un quadro che integri le loro pratiche di lavoro esistenti, purché tenga conto degli elementi costitutivi di cui all'articolo 35, paragrafo 7. Tale quadro può essere personalizzato per lo specifico titolare del trattamento oppure essere comune a un determinato settore. I quadri precedentemente pubblicati sviluppati dalle autorità di protezione dei dati dell'UE e i quadri specifici di settore dell'UE includono (elenco non esaustivo):

esempi di quadri generici dell'UE:

- DE: modello per la protezione dei dati standard, V.1.0 - versione di prova, 2016[31]. https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf;
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf;
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015. https://www.cnil.fr/fr/node/15798;
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf;

esempi di quadri UE specifici di settore:

- *Privacy and Data Protection Impact Assessment Framework for RFID Applications* [Quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati per le applicazioni RFID][32]. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf;
- *Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems* [Modello per la valutazione d'impatto sulla protezione dei dati per la rete intelligente e i sistemi di misurazione intelligenti][33]

---

[31] Approvato all'unanimità e affermativamente (con l'astensione della Baviera) dalla 92ª conferenza delle autorità indipendenti per la protezione dei dati del *Bund* e dei *Länder* di Kühlungsborn tenutasi il 9 e 10 novembre 2016.

[32] Cfr. anche:

- Raccomandazione della Commissione, del 12 maggio 2009, sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza. http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32009H0387&from=IT;
- Parere 9/2011 sulla proposta rivista dell'industria relativa a un quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati per le applicazioni RFID. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_it.pdf.

[33] Cfr. anche il "Parere 07/2013 concernente il modello di valutazione d'impatto sulla protezione dei dati per la rete intelligente e i sistemi di misurazione intelligenti ("modello di valutazione d'impatto sulla protezione dei dati") elaborato dal gruppo di esperti n. 2 della task force della Commissione per le reti intelligenti.

http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf.

Anche una norma internazionale fornirà orientamenti in merito alle metodologie utilizzate per la realizzazione di una valutazione d'impatto sulla protezione dei dati (ISO/IEC 29134[34]).

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_it.pdf.

[34] ISO/IEC 29134 (progetto), *Information technology – Security techniques – Privacy impact assessment – Guidelines* (in inglese), Organizzazione internazionale per la normazione (ISO).

Allegato 2 - Criteri per una valutazione d'impatto sulla protezione dei dati accettabile

Il WP29 propone i seguenti criteri che i titolari del trattamento possono utilizzare per stabilire se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno oppure se una metodologia per lo svolgimento di una tale valutazione sia sufficientemente completa per garantire il rispetto del regolamento generale sulla protezione dei dati:

- ☐ una descrizione sistematica del trattamento è fornita (articolo 35, paragrafo 7, lettera a)):
  - ☐ la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);
  - ☐ vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
  - ☐ viene fornita una descrizione funzionale del trattamento;
  - ☐ sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);
  - ☐ si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);
- ☐ la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):
  - ☐ sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):
    - ☐ misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
      - ☐ finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));
      - ☐ liceità del trattamento (articolo 6);
      - ☐ dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));
      - ☐ limitazione della conservazione (articolo 5, paragrafo 1, lettera e));
    - ☐ misure che contribuiscono ai diritti degli interessati:
      - ☐ informazioni fornite all'interessato (articoli 12, 13 e 14);
      - ☐ diritto di accesso e portabilità dei dati (articoli 15 e 20);
      - ☐ diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);
      - ☐ diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);
      - ☐ rapporti con i responsabili del trattamento (articolo 28);
      - ☐ garanzie riguardanti trattamenti internazionali (capo V);
      - ☐ consultazione preventiva (articolo 36).
- ☐ i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c)):
  - ☐ l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:
    - ☐ si considerano le fonti di rischio (considerando 90);
    - ☐ sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
    - ☐ sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;
    - ☐ sono stimate la probabilità e la gravità (considerando 90);
  - ☐ sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);
- ☐ le parti interessate sono coinvolte:
  - ☐ si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);
  - ☐ si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).