17/EN
WP 248

Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679

Adottate il 4 aprile 2017
Versione successivamente emendata e adottata il 4 ottobre 2017

INDICE

I. Introduzione

II. Oggetto

III. DPIA: cosa prevede il regolamento

A. Qual è l'oggetto della DPIA? Un singolo trattamento ovvero un insieme di trattamenti simili
B. Quali trattamenti sono soggetti a DPIA? Salvo eccezioni, qualora un trattamento "possa presentare un rischio elevato".
    a. *Quando sussiste l'obbligo di condurre una DPIA? Qualora un trattamento "possa presentare un rischio elevato"*
    b. *Quando non è necessario condurre una DPIA? Quando il trattamento non "può comportare un rischio elevato", o esiste una DPIA analoga, o è già stato autorizzato prima del maggio 2018, o ha una base legale, o compare nell'elenco dei trattamenti per i quali non è richiesta una DPIA*
C. Per quanto riguarda i trattamenti già in corso? Una DPIA è richiesta in talune circostanze
D. Come si effettua una DPIA?
    a. *Quando è opportuno condurre la DPIA? Prima di procedere al trattamento*
    b. *Chi è tenuto a condurre la DPIA? Il titolare, insieme al RPD e al responsabile (o ai responsabili) del trattamento*
    c. *Quale metodologia deve essere applicata per condurre una DPIA? Vi possono essere metodologie diverse, ma i criteri devono essere gli stessi*
    d. *È obbligatorio pubblicare la DPIA? No, ma pubblicarne una sintesi può promuovere un rapporto fiduciario, e la documentazione integrale della DPIA deve essere trasmessa all'autorità di controllo in caso di consultazione preventiva ovvero su richiesta dell'autorità stessa*
E. Quando occorre consultare l'autorità di controllo? Se i rischi residuali sono elevati

IV. Conclusioni e raccomandazioni

Allegato 1 – Esempi di schemi di DPIA attualmente esistenti nell'Ue

Allegato 2 – Criteri riferiti a una DPIA accettabile

IL GRUPPO DI LAVORO SULLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli Articoli 29 e 30 della stessa,

visto il proprio regolamento,

HA ADOTTATO LE PRESENTI LINEE-GUIDA:

I. Introduzione

Il regolamento 2016/679[1] (RGPD) sarà applicabile a partire dal 25 maggio 2018. L'art. 35 del RGPD introduce la nozione di valutazione di impatto sulla protezione dei dati (DPIA, utilizzando l'acronimo inglese per *Data Protection Impact Assessment*)[2], e lo stesso dicasi per la direttiva 2016/680[3].

Una DPIA consiste in una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali[4] (attraverso la valutazione di tali rischi e la definizione delle misure idonee ad affrontarli). 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 a dimostrare l'adozione di misure idonee a garantire il rispetto di

---

[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 di 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 si trova spesso utilizzato anche l'acronimo "PIA" (*Privacy Impact Assessment*, ossia Valutazione di impatto sulla privacy), con identico riferimento concettuale.

[3] Anche in base all'art. 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 di 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 e che abroga la decisione quadro 2008/977/GAI del Consiglio, è necessario effettuare una valutazione di impatto sulla protezione dei dati con riguardo a un trattamento che "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*".

[4] Nel regolamento non si individua una definizione formale di DPIA in quanto tale, tuttavia

- i contenuti minimi della DPIA sono specificati come segue all'art. 35, paragrafo 7:
  - "*a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;*
  - *b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;*
  - *c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;*
  - *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 valore e il ruolo della DPIA sono chiariti nel Considerando 84 nei termini seguenti: "*Per 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.*"

tali prescrizioni (si veda anche l'art. 24)[5]. In altri termini, **la DPIA è una procedura che permette di realizzare e dimostrare la conformità con le norme**.

In base al regolamento, l'inosservanza degli obblighi concernenti la DPIA può comportare l'imposizione di sanzioni pecuniarie da parte della competente autorità di controllo. Il mancato svolgimento della DPIA quando il trattamento è soggetto a tale valutazione (art. 35, paragrafi 1 e 3-4), lo svolgimento non corretto di una DPIA (art. 35, paragrafi 2 e 7-9) o la mancata consultazione dell'autorità di controllo competente ove ciò sia necessario (art. 36, paragrafo 3, lettera e)) possono comportare l'irrogazione di una sanzione amministrativa pecuniaria fino a un massimo di 10 milioni di Euro, ovvero – se si tratta di un'impresa – fino al 2% del fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore.

II. Oggetto

Le presenti linee-guida tengono conto di quanto segue:

- la dichiarazione del Gruppo di lavoro "Articolo 29" (WP29), 14/EN WP218[6];
- le linee-guida del WP29 in materia di responsabili della protezione dei dati (RPD/DPO), 16/EN WP243;[7]
- il parere del WP29 sul principio di limitazione della finalità, 13/EN WP2013[8];
- standard internazionali[9].

Coerentemente con l'approccio basato sul rischio che informa l'intero RGPD, lo svolgimento di una DPIA non è obbligatorio per ogni singolo trattamento. La DPIA è necessaria solo se il trattamento "può comportare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35, paragrafo 1). Al fine di assicurare un'interpretazione coerente dei casi di obbligatorietà della DPIA (art. 35, paragrafo 3), le presenti linee-guida vogliono chiarire, in primo luogo, il concetto stesso di DPIA e fornire, quindi, alcuni criteri in vista dell'elaborazione degli elenchi che le autorità di controllo sono tenute ad adottare in base all'art. 35, paragrafo 4.

Ai sensi dell'art. 70, paragrafo 1, lettera e), il Comitato europeo per la protezione dei dati (CEPD) potrà pubblicare linee-guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del RGPD. Scopo del presente documento è precorrere questa funzione attribuita al CEPD e, quindi, chiarire le pertinenti disposizioni del regolamento così da contribuire all'osservanza delle norme da parte dei titolari e assicurare certezza del diritto per quei titolari che siano tenuti a svolgere una DPIA.

Le linee-guida vogliono, inoltre, favorire la definizione di

---

[5] Si veda 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*."

[6] Dichiarazione del WP29 (14/EN WP218) relativa al ruolo di un approccio basato sul rischio nel quadro normativo in materia di protezione dati, adottata il 30 maggio 2014 - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[7] Linee-guida del WP29 sui responsabili della protezione dei dati, 16/EN WP243, adottate il 13 dicembre 2016 - http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

[8] Parere 3/2013 del WP29 sul principio di limitazione della finalità, 13/EN WP203, adottato il 2 aprile 2013 - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[9] Per esempio ISO 31000:2009, *Risk management – Principles and guidelines,* International Organization for Standardization (ISO); ISO/IEC 20134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines,* International Organization for Standardization (ISO).

- un elenco condiviso a livello Ue di trattamenti per i quali la DPIA è obbligatoria (art. 35, paragrafo 4);
- un elenco condiviso a livello Ue di trattamenti per i quali la DPIA non è necessaria (art. 35, paragrafo 5);
- criteri condivisi rispetto alla metodologia di svolgimento della DPIA (art. 35, paragrafo 5);
- criteri condivisi rispetto ai casi di consultazione obbligatoria dell'autorità di controllo (art. 36, paragrafo 1);
- raccomandazioni, ove possibile fondate sull'esperienza raccolta negli Stati membri dell'Ue.

III. DPIA: cosa prevede il regolamento

Il regolamento impone ai titolari di mettere in atto misure idonee a garantire ed essere in grado di dimostrare l'osservanza del regolamento stesso, tenendo conto, fra gli altri, dei "*rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*" (art. 24, paragrafo 1). L'obbligo di condurre una DPIA, in determinate circostanze, deve essere collocato nel contesto del più generale obbligo imposto ai titolari di gestire correttamente i rischi connessi al trattamento di dati personali.

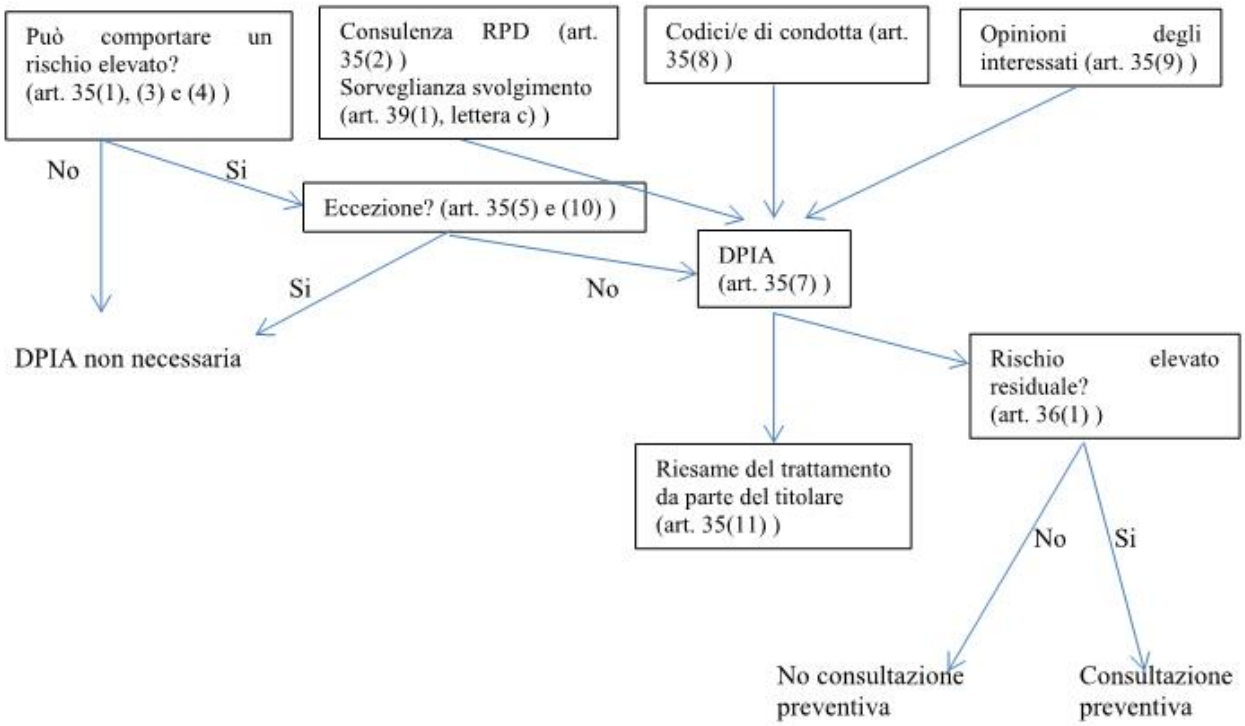
Per "rischio" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità. D'altro canto, la "gestione del rischio" è definibile come l'insieme coordinato delle attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio.

L'art. 35 del regolamento menziona la probabilità di un rischio elevato "*per i diritti e le libertà delle persone fisiche*".

Come già chiarito dal Gruppo di lavoro "Articolo 29" nella "Dichiarazione" sul ruolo di un approccio basato sul rischio nel contesto giuridico della protezione dei dati, il riferimento ai "diritti e le libertà" degli interessati va inteso in primo luogo come relativo al diritto alla privacy, ma può riguardare anche altri diritti fondamentali quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.

Coerentemente con l'approccio basato sul rischio che informa il regolamento, non è obbligatorio condurre una DPIA per ogni singolo trattamento. Viceversa, la DPIA è obbligatoria solo se una determinata tipologia di trattamenti "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (art. 35, paragrafo 1). Tuttavia, la semplice circostanza per cui non siano soddisfatte le condizioni che generano un obbligo di condurre la DPIA non riduce in alcun modo l'obbligo più generale cui soggiacciono i titolari di mettere in atto misure finalizzate a gestire in modo idoneo i rischi per i diritti e le libertà degli interessati. Nella pratica, ciò significa che i titolari devono valutare in modo continuativo i rischi creati dai propri trattamenti così da individuare quelle situazioni in cui una determinata tipologia di trattamenti "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*".

La figura seguente illustra i principi fondamentali concernenti la DPIA in base al RGPD:



A. Qual è l'oggetto della DPIA? Un singolo trattamento ovvero un insieme di trattamenti simili

Una DPIA può riguardare un singolo trattamento; tuttavia, l'art. 35, paragrafo 1, prevede che "*Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*", e il considerando 92 aggiunge che "*Vi 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*".

È **possibile utilizzare un'unica DPIA per valutare più trattamenti che presentano analogie** in termini di natura, ambito, contesto, finalità e rischi. In effetti, le valutazioni di impatto mirano a svolgere un'analisi sistematica di situazioni nuove che potrebbero comportare rischi elevati per i diritti e le libertà delle persone fisiche, e non occorre condurre una DPIA per quei trattamenti - svolti in un contesto specifico e per una specifica finalità – che siano già stati oggetto di analisi. Un esempio potrebbe essere offerto dall'utilizzo di tecnologie simili per raccogliere le stesse tipologie di dati per le identiche finalità; si pensi a un gruppo di autorità locali che decidano di installare ciascuna un analogo sistema di videosorveglianza: sarebbe possibile svolgere un'unica DPIA che prenda in esame il trattamento svolto da questi distinti titolari; oppure si pensi a un operatore ferroviario (unico titolare del trattamento) che potrebbe svolgere un'unica DPIA con riguardo all'impiego della videosorveglianza in tutte le stazioni ferroviarie di competenza. Lo stesso dicasi per trattamenti analoghi effettuati da titolari diversi; in casi del genere, sarebbe opportuno che una

DPIA utilizzabile come riferimento venga condivisa o resa accessibile al pubblico, con l'obbligo di dare attuazione alle misure in essa delineate, mentre si dovrebbe giustificare la scelta di condurre una DPIA isolata.

Quando un trattamento è svolto in contitolarità, è necessario che ciascun contitolare definisca con precisione gli obblighi rispettivamente incombenti. La DPIA dovrebbe stabilire chi ha la responsabilità delle singole misure finalizzate alla gestione dei rischi e alla tutela dei diritti e delle libertà degli interessati. Ciascun titolare dovrebbe indicare con chiarezza le rispettive esigenze e condividere tutte le informazioni utili senza pregiudicare quanto coperto da segreto (per esempio, informazioni tutelate dal segreto commerciale, soggette a diritti di proprietà intellettuale, informazioni economiche riservate) né rivelare eventuali vulnerabilità.

Una DPIA può rivelarsi utile anche per valutare l'impatto di un nuovo dispositivo tecnologico in termini di protezione dei dati; è il caso, per esempio, di un nuovo prodotto hardware o software, se utilizzabile da titolari diversi per svolgere trattamenti diversi. Naturalmente il titolare che utilizzi tale prodotto resta tenuto a condurre una distinta DPIA rispetto alla specifica implementazione, ma – ove opportuno – tale DPIA può essere informata alla DPIA predisposta dal fornitore del prodotto. A titolo di esempio, si pensi al rapporto che sussiste fra produttori di contatori intelligenti e società fornitrici di elettricità. Ciascun fornitore del prodotto come anche ciascun soggetto che effettui trattamenti attraverso tale prodotto dovrebbe condividere ogni informazione utile senza pregiudicare quanto è protetto da segreto né generare rischi in termini di sicurezza a causa della rivelazione di eventuali vulnerabilità.

B. Quali trattamenti sono soggetti a DPIA? Quelli che "*possono presentare un rischio elevato*", salve eccezioni

In questo paragrafo si esaminano i casi in cui la DPIA è obbligatoria e quelli in cui essa non è necessaria.

A meno che il trattamento ricada nelle eccezioni previste (III.B.b.), la DPIA deve essere condotta qualora un trattamento "possa presentare un rischio elevato" (III.B.a).

a) Quando sussiste l'obbligo di condurre una DPIA? Qualora un trattamento "*possa presentare un rischio elevato*"

Il regolamento non impone di condurre una DPIA con riguardo a ogni trattamento che possa comportare rischi per i diritti e le libertà delle persone fisiche. La DPIA è obbligatoria solo qualora un trattamento "*possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (art. 35, paragrafo 1), come meglio chiarito dal paragrafo 3 dell'art. 35 e integrato da quanto prevede il paragrafo 4 dello stesso articolo. Si tratta di un requisito particolarmente pertinente qualora si intenda introdurre una tecnologia di trattamento innovativa.[10]

Se la necessità di una DPIA non emerge con chiarezza, il WP29 raccomanda di farvi comunque ricorso in quanto la DPIA contribuisce all'osservanza delle norme in materia di protezione dati da parte dei titolari di trattamento.

Benché una DPIA possa risultare necessaria in altre circostanze, l'art. 35, paragrafo 3, cita alcuni esempi di trattamenti che "*possono risultare in un rischio elevato*":

[10] Si vedano i considerando 89, 91 e l'art. 35, paragrafi (1) e (3), quanto a esemplificazioni ulteriori.

"(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[11]*;*
- (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[12]*; o*
- (c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".

Come segnalato dall'utilizzo della locuzione "in particolare" nel paragrafo 3 dell'art. 35, l'elenco di cui sopra non ha pretese di esaustività. Possono esservi trattamenti "a rischio elevato" che non sono ricompresi nell'elenco in questione, pur comportando rischi elevati in misura analoga. Anche questi trattamenti dovrebbero essere oggetto di DPIA. Per tale motivo, i criteri elaborati nel prosieguo si spingono talora oltre la mera illustrazione di cosa debba intendersi in rapporto ai tre esempi forniti nell'art. 35, paragrafo 3, del regolamento.

Allo scopo di fornire indicazioni più concrete rispetto ai trattamenti che richiedono una DPIA a causa del rischio inerentemente elevato, e tenendo conto degli elementi specifici contenuti negli articoli 35, paragrafo 1, e 35, paragrafo 3, lettere a)-c), nonché degli elenchi di cui è prevista l'adozione a livello nazionale in base all'art. 35, paragrafo 4, dei considerando 71, 75 e 91, e degli altri riferimenti contenuti nel regolamento a trattamenti "*che possono presentare un rischio elevato*"[13], è opportuno prendere in esame i seguenti nove criteri:

1. Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, in particolare a partire da "*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). A titolo esemplificativo si possono citare un istituto finanziario che effettui lo screening dei propri clienti utilizzando un database di rischio creditizio ovvero un database per la lotta alle frodi o al riciclaggio e al finanziamento del terrorismo (AML/CTF); una società operante nel settore delle biotecnologie che offra test genetici direttamente ai consumatori per finalità predittive del rischio di determinate patologie o in generale per lo stato di salute; una società che crei profili comportamentali o di marketing a partire dalle operazioni o dalla navigazione compiute sul proprio sito web.
2. Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura: trattamenti finalizzati ad assumere decisioni su interessati che producano "*effetti giuridici sulla persona fisica*" ovvero che "*incidono in modo analogo significativamente su dette persone fisiche*" (art. 35, paragrafo 3, lettera a)). Per esempio, il trattamento può comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione. Il trattamento che produce effetti minimi o nulli su un interessato non soddisfa questo specifico criterio. Per maggiori dettagli sui concetti in gioco si rimanda alle Linee-guida in materia di profilazione che il Gruppo di lavoro si appresta a pubblicare.
3. Monitoraggio sistematico: trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o "*la sorveglianza sistematica di*

[11] Si veda il considerando 71: "*in particolare al fine di analizzare o prevedere 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*".
[12] Si veda il 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".*
[13] Si vedano, per esempio, i considerando 75, 76, 92, 116.

un'area accessibile al pubblico" (art. 35, paragrafo 3, lettera c)).[14] Questa tipologia di monitoraggio costituisce un criterio, ai fini della DPIA, in quanto la raccolta di dati personali può avvenire in circostanze tali da non consentire agli interessati di comprendere chi vi stia procedendo e per quali finalità. Inoltre, è talora impossibile per gli interessati sottrarsi a questa tipologia di trattamenti in aree pubbliche (o pubblicamente accessibili).

4. Dati sensibili o dati di natura estremamente personale: si tratta delle categorie particolari di dati personali di cui all'art. 9 (per esempio, informazioni sulle opinioni politiche di una persona fisica) oltre ai dati personali relativi a condanne penali o reati di cui all'art. 10. A titolo di esempio, si può citare un ospedale che conserva le cartelle cliniche dei pazienti, o un investigatore privato che conserva informazioni su soggetti responsabili di reati. Al di là di queste disposizioni del regolamento, vi sono talune categorie di dati che possono aumentare i rischi eventuali per i diritti e le libertà delle persone fisiche. Si tratta di dati personali considerati sensibili (nell'accezione comune del termine), in quanto connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza) ovvero in quanto incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) ovvero in quanto una loro violazione comporta evidentemente un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti). A tale proposito, può essere pertinente la circostanza per cui i dati siano già stati resi pubblici dall'interessato ovvero da terzi. Il fatto che un certo dato personale sia disponibile pubblicamente può essere un elemento da prendere in esame nel valutare l'aspettativa di un utilizzo ulteriore di tale dato per determinati scopi. Il criterio in oggetto può riferirsi anche a dati quali documenti personali, email, agende, appunti tratti da lettori elettronici dotati di dispositivi per la presa di appunti, e informazioni molto personali contenute in applicazioni che consentono di tenere traccia del proprio stile di vita.
5. Trattamenti di dati su larga scala: il regolamento non offre definizioni del concetto di "larga scala", anche se il considerando 91 fornisce indicazioni in merito. In ogni caso, il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori seguenti al fine di stabilire se un trattamento sia svolto su larga scala[15]:
    a. numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento;
    b. volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento;
    c. durata, o persistenza, dell'attività di trattamento;
    d. ambito geografico dell'attività di trattamento.
6. Combinazione o raffronto di insiemi di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato.[16]
7. Dati relativi a interessati vulnerabili (considerando 75): il trattamento di questa tipologia di informazioni rappresenta un criterio ai fini della DPIA in quanto è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento, nel senso che il singolo può non

---

[14] L'interpretazione del termine "sistematico" fornita dal WP29 (si vedano le "Linee-guida sul responsabile della protezione dei dati" (16/EN WP243)) è la seguente:

- 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 WP29 interpreta l'espressione "area accessibile al pubblico" nel senso di un luogo aperto alla generalità delle persone, per esempio una piazza, un centro commerciale, una strada, una biblioteca pubblica.

[15] Si vedano le Linee-guida del WP29 in materia di responsabili della protezione dei dati 16/EN WP243.

[16] Si veda l'analisi svolta nel parere del WP29 sul principio di limitazione della finalità 13/EN WP203, p. 24.

disporre del potere di acconsentire, o di opporsi, con facilità al trattamento dei propri dati, né può talora con facilità esercitare i propri diritti. La categoria degli interessati vulnerabili comprende anche i minori, che. si può ritenere non siano in grado di opporsi o acconsentire, in modo consapevole e ragionato, al trattamento dei propri dati personali, i dipendenti, quei segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela (soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti) e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.

8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative, come l'associazione fra tecniche dattiloscopiche e riconoscimento del volto per migliorare il controllo degli accessi fisici, e così via. Il regolamento chiarisce (art. 35, paragrafo 1, e considerando 89 e 91) che l'utilizzo di una nuova tecnologia, definito "*in conformità con il grado di conoscenze tecnologiche raggiunto*" (considerando 91), può comportare l'obbligo di condurre una DPIA, in quanto il ricorso a una nuova tecnologia può generare forme innovative di raccolta e utilizzo dei dati cui può associarsi un rischio elevato per i diritti e le libertà delle persone. Nei fatti, le conseguenze sul piano individuale e sociale del ricorso a una nuova tecnologia sono talora ignote. La DPIA aiuterà il titolare a comprendere e gestire tali rischi. Per esempio, alcune applicazioni legate all' "Internet delle cose" potrebbero avere impatti significativi sulla vita privata e le abitudini delle persone, e, quindi, necessitano di una DPIA.
9. Tutti quei trattamenti che, di per sé, "*impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto*" (art. 22 e considerando 91). Ciò comprende i trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o la stipulazione di un contratto. Si pensi, a titolo di esempio, allo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento.

Un titolare può ritenere, nella maggioranza dei casi, che quando un trattamento soddisfa due dei criteri sopra indicati sia necessario condurre una DPIA. In linea di principio, il Gruppo di lavoro ritiene che quanto maggiore è il numero dei criteri soddisfatti da un determinato trattamento, tanto maggiore è la probabilità che esso presenti un rischio elevato per i diritti e le libertà degli interessati e, quindi, che si renda necessaria una DPIA indipendentemente dalle misure che il titolare prevede di adottare.

Tuttavia, in taluni casi **un titolare può ritenere che un trattamento che soddisfa solo uno dei criteri di cui sopra necessiti di una DPIA**.

Gli esempi riportati di seguito illustrano come utilizzare i criteri in oggetto per valutare se un determinato trattamento richieda la conduzione di una DPIA:

Esempi di trattamento	**Criteri pertinenti**	**Obbligo di DPIA probabile?**
Ospedale che tratta dati genetici e sanitari relativi ai pazienti (sistema informativo ospedaliero)	• Dati sensibili o dati di natura estremamente personale • Dati relativi a interessati vulnerabili • Dati trattati su larga scala	
Utilizzo di un sistema di	• Monitoraggio	

videosorveglianza per il controllo del traffico autostradale. Il titolare prevede di utilizzare un sistema intelligente di analisi delle immagini per l'individuazione dei veicoli e il riconoscimento automatico delle targhe	sistematico • Utilizzi innovativi o applicazione di soluzioni tecnologiche o organizzative	Sì
Azienda che controlla sistematicamente le attività dei dipendenti, compreso l'utilizzo dei terminali informatici, la navigazione su Internet, ecc.	• Monitoraggio sistematico • Dati relativi a interessati vulnerabili	
Raccolta di dati pubblici tratti dai *social media* per la creazione di profili	• Valutazione o scoring • Dati trattati su larga scala • Raffronto o combinazione di insiemi di dati • Dati sensibili o dati di natura estremamente personale	
Un'istituzione che crei un database nazionale di valutazioni creditizie o per finalità antifrode	• Valutazione o scoring • Decisioni automatizzate che producono effetti giuridici o incidono in modo analogo sull'interessato in misura significativa • Impedimenti all'esercizio di un diritto o all'utilizzo di un servizio o di un contratto da parte dell'interessato • Dati sensibili o dati di natura estremamente personale	
Conservazione per scopi di archiviazione di dati sensibili pseudonimizzati relativi a interessati vulnerabili coinvolti in progetti di ricerca o studi clinici sperimentali	• Dati sensibili • Dati relativi a interessati vulnerabili • Impedimenti all'esercizio di un diritto o all'utilizzo di un servizio o di un contratto da parte dell'interessato	
Trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" (considerando 91)	• Dati sensibili o dati di natura estremamente personale • Dati relativi a interessati vulnerabili	No
Rivista online che utilizza una mailing list	• Dati trattati su larga	

per inviare agli abbonati un bollettino giornaliero di carattere generale	scala	
Sito di e-commerce che pubblicizza parti di ricambio per auto d'epoca con limitata profilazione riferita ad alcune sezioni del sito e basata sui pregressi acquisti effettuati	• Valutazione o scoring	

Viceversa, può darsi il caso di un trattamento che riflette gli esempi sopra indicati ma che, a giudizio del titolare, non "può presentare un rischio elevato". In casi del genere, il titolare dovrà motivare e documentare la scelta della mancata conduzione della DPIA, allegando o annotando l'opinione del responsabile della protezione dei dati.

Inoltre, il principio di responsabilizzazione prevede che ciascun titolare "*tiene un registro delle attività di trattamento svolte sotto la propria responsabilità*" comprendente, fra l'altro, le finalità del trattamento, una descrizione delle categorie di dati e i destinatari dei dati stessi, nonché "*ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1*" (art. 30, paragrafo 1) e deve valutare se vi sia la probabilità di un rischio elevato anche se potrà decidere, in ultima analisi, di non condurre una DPIA.

Nota: Le autorità di controllo sono tenute a redigere, pubblicare e comunicare al Comitato europeo per la protezione dei dati (CEPD) un elenco dei trattamenti che necessitano di una DPIA (art. 35, paragrafo 4).[17] I criteri sopra indicati possono facilitare la definizione di tale elenco da parte delle autorità di controllo, che potranno eventualmente aggiungere elementi più specifici col tempo. Per esempio, anche il trattamento di qualsiasi tipologia di dato biometrico o di dati relativi a minori potrebbe essere considerato pertinente ai fini dell'inserimento nell'elenco di cui all'art. 35, paragrafo 4.

b) Quando non è necessario condurre una DPIA? Quando il trattamento non "*può comportare un rischio elevato*" o esiste una DPIA simile, o il trattamento è già stato autorizzato prima del maggio 2018, o ha una base legale [SIC], o è compreso nella lista dei trattamenti che non richiedono una DPIA.

Il Gruppo di lavoro ritiene che una DPIA non sia necessaria nei casi seguenti:

- **se il trattamento non "*può comportare un rischio elevato per i diritti e le libertà di persone fisiche*"** (art. 35, paragrafo 1);
- **se la natura, l'ambito, il contesto e le finalità del trattamento sono molto simili a quelli del trattamento per cui è già stata condotta una DPIA**. In casi del genere, si possono utilizzare i risultati della DPIA per trattamenti analoghi (art. 35, paragrafo 1);[18]
- se il trattamento è stato sottoposto a verifica da parte di un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche[19] (v. III.C);

[17] Al riguardo, "*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*" (art. 35, paragrafo 6).

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

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

- **se un trattamento**, conformemente con la lettera c) o e) dell'articolo 6, paragrafo 1, **trova la propria base legale** nel diritto dell'Ue o di uno Stato membro, la base legale in questione disciplina lo specifico trattamento, **ed è già stata condotta una DPIA** all'atto della definizione della base giuridica suddetta (art. 35, paragrafo 10)[20], tranne ove uno Stato membro abbia previsto la necessità di condurre una DPIA per i trattamenti pregressi;
- **se il trattamento è compreso nell'elenco facoltativo (redatto dall'autorità di controllo ai sensi dell'art. 35, paragrafo 5) dei trattamenti** per i quali non è necessario procedere alla DPIA. Tale elenco può riguardare trattamenti conformi alle condizioni specificate dalla singola autorità, in particolare attraverso linee-guida, decisioni o autorizzazioni specifiche, norme di conformità, ecc. (per esempio, in Francia, attraverso autorizzazioni, deroghe, norme semplificate, pacchetti di conformità, ecc.). In casi del genere, salvo riesame da parte della competente autorità di controllo, la DPIA non è necessaria – ma solo a condizione che il trattamento ricada nello specifico ambito della procedura menzionata nell'elenco e continui a risultare pienamente conforme ai relativi requisiti del regolamento.

C) Per quanto riguarda i trattamenti già in corso? Una DPIA è necessaria in talune circostanze.

L'obbligo di condurre una DPIA vige per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e per i quali siano intervenute variazioni dei rischi tenuto conto della natura, dell'ambito, del contesto e delle finalità dei trattamenti stessi.

Non è necessario condurre una DPIA per quei trattamenti che siano stati oggetto di verifica preliminare da parte di un'autorità di controllo o da un responsabile della protezione dei dati(*) e che proseguano con le stesse modalità oggetto di tale verifica. Come indicato nel considerando 171, "*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*".

Viceversa, ciò significa che tutti i trattamenti le cui caratteristiche attuative (ambito, finalità, dati personali raccolti, identità di titolari o destinatari, periodi di conservazione dei dati, misure tecniche e organizzative, ecc.) sono mutate rispetto alla valutazione preliminare svolta dall'autorità di controllo o da un responsabile della protezione dei dati(*), e che possono presentare un rischio elevato, dovrebbero essere oggetto di una DPIA. Inoltre, la necessità di una DPIA potrebbe insorgere al modificarsi dei rischi derivanti dai trattamenti, [21] per esempio a causa del ricorso a una nuova tecnologia oppure dell'utilizzo dei dati personali per una diversa finalità.

I trattamenti tendono a evolvere rapidamente e possono facilmente presentarsi nuove vulnerabilità; pertanto, occorre osservare che la revisione di una DPIA non è soltanto utile ai fini del miglioramento continuo, ma è anche indispensabile per mantenere inalterato il livello di protezione dei dati al mutare delle condizioni nel tempo.

---

[20] Si osservi che, qualora sia stata condotta una DPIA nella fase di elaborazione dello strumento che offre la base legale per il trattamento, è probabile che sia necessario un riesame prima dell'entrata in vigore poiché lo strumento giuridico adottato può differire da quello proposto in misura tale da incidere sull'impatto in termini di privacy e protezione dei dati. Inoltre, può darsi che non siano disponibili sufficienti informazioni di ordine tecnico rispetto al trattamento in quanto tale al momento dell'adozione dello strumento normativo suddetto, anche se accompagnato da una DPIA; in casi del genere, può risultare comunque necessario condurre una DPIA specifica prima di procedere al trattamento vero e proprio.

(*) Nel nostro paese, l'unico soggetto che dispone di tale potere è il Garante.

[21] In termini di contesto, dati raccolti, funzionalità, dati personali oggetto di trattamento, destinatari, incroci di dati, rischi (beni di supporto, fonti di rischio, impatti potenziali, minacce, ecc.), misure di sicurezza e trasferimenti internazionali.

Una DPIA può rendersi necessaria per il mutamento del contesto organizzativo o sociale relativo a uno specifico trattamento; è il caso, per esempio, degli effetti prodotti da decisioni automatizzate, che possono acquistare maggiore significatività, oppure del presentarsi di nuove categorie di interessati vulnerabili alla discriminazione. Ciascuno di tali esempi potrebbe costituire un elemento in grado di modificare il rischio derivante dallo specifico trattamento.

Peraltro, alcune variazioni potrebbero dare luogo di fatto a una diminuzione del rischio. Per esempio, un trattamento potrebbe evolvere nel senso di non comportare più decisioni automatizzate, oppure un'attività di monitoraggio potrebbe cessare di essere sistematica. In tal caso, il riesame dell'analisi dei rischi precedentemente condotta può indicare che non sussiste più la necessità di condurre una DPIA.

In termini di buone prassi, per i trattamenti in corso dovrebbe essere previsto un riesame continuo della DPIA, **ripetendo la valutazione a intervalli regolari.** Pertanto, anche qualora non vi sia l'obbligo di condurre una DPIA al 25 maggio 2018, sarà necessario che il titolare, al momento opportuno, conduca tale DPIA nel quadro degli obblighi più generali di responsabilizzazione cui ogni titolare soggiace.

D. Come si effettua una DPIA?

a) Quando è opportuno condurre la DPIA? Prima di procedere al trattamento

La DPIA dovrebbe essere condotta "*prima di procedere al trattamento*" (art. 35, paragrafo 1, e art. 35, paragrafo 10; considerando 80 e 93).[22]. Tale impostazione è coerente con i principi di protezione dei dati sin dalla fase di progettazione e per impostazione predefinita (art. 25 e considerando 78). La DPIA deve essere considerata uno strumento di ausilio nel processo decisionale relativo al trattamento.

L'effettuazione della DPIA dovrebbe collocarsi quanto più a monte possibile nella fase di progettazione di un trattamento, anche se non tutte le operazioni di tale trattamento sono già delineate. L'aggiornamento della DPIA nel corso dell'intero ciclo di vita di un determinato progetto garantirà la dovuta considerazione delle tematiche di privacy e protezione dei dati favorendo l'individuazione di soluzioni che promuovano l'osservanza. Talora potrà rendersi necessaria la ripetizione di singole tappe della valutazione con il procedere della fase di sviluppo, in quanto la scelta di determinate misure tecniche o organizzative potrà incidere sulla gravità o sulla probabilità dei rischi posti dal trattamento.

Il fatto che possa rendersi necessario un aggiornamento della DPIA dopo l'inizio effettivo del trattamento non è una buona ragione per differire o evitare di condurre una DPIA. La DPIA è un processo permanente, soprattutto se si ha a che fare con un trattamento dinamico e soggetto a continue trasformazioni. **Lo svolgimento della DPIA è un processo continuativo e non un'attività *una tantum*.**

b) Chi è tenuto a condurre la DPIA? Il titolare, insieme al RPD e al responsabile (o ai responsabili) del trattamento

[22] Tranne in presenza di un trattamento già in corso sottoposto a verifica preliminare da parte dell'autorità di controllo, nel qual caso la DPIA dovrebbe essere condotta prima di apportare modifiche significative al trattamento stesso.

Spetta al titolare garantire l'effettuazione della DPIA (art. 35, paragrafo 2). La conduzione materiale della DPIA può essere affidata a un altro soggetto, interno o esterno all'organismo; tuttavia, la responsabilità ultima dell'adempimento ricade sul titolare del trattamento.

Il titolare deve consultarsi con il responsabile della protezione dei dati (RPD/DPO), ove designato (art. 35, paragrafo 2); tale consultazione e le conseguenti decisioni assunte dal titolare devono essere documentate nell'ambito della DPIA. Il RPD è chiamato anche a monitorare lo svolgimento della DPIA (art. 39, paragrafo 1, lettera c)). Indicazioni ulteriori sono rinvenibili nelle linee-guida del WP29 sul responsabile della protezione dei dati (16/EN WP243).

Se il trattamento è svolto, in tutto o in parte, da un responsabile, **quest'ultimo deve assistere il titolare nella conduzione della DPIA** fornendo ogni informazione necessaria conformemente con l'art. 28, paragrafo 3, lettera f).

Il titolare "*raccoglie le opinioni degli interessati o dei loro rappresentanti*" "*se del caso*" (art. 35, paragrafo 9). A giudizio del WP29,

- per la raccolta delle opinioni in oggetto si possono individuare molteplici modalità, in rapporto al contesto: per esempio, uno studio generico relativo a finalità e mezzi del trattamento; un quesito rivolto ai rappresentanti del personale; un questionario inviato ai futuri clienti del titolare Il titolare dovrà aver cura di accertarsi dell'esistenza di una base legale per il trattamento di dati personali eventualmente connesso alla raccolta di tali opinioni. Occorre rilevare, tuttavia, che il consenso al trattamento in questione non rappresenta ovviamente una modalità idonea per raccogliere le opinioni degli interessati;
- qualora la decisione assunta in ultima analisi dal titolare si discosti dall'opinione degli interessati, è bene che il titolare documenti le motivazioni che hanno condotto alla prosecuzione o meno del progetto;
- il titolare dovrebbe documentare anche le motivazioni della mancata consultazione degli interessati, qualora decida che quest'ultima non sia opportuna – per esempio, perché potrebbe pregiudicare la riservatezza dei piani aziendali, oppure sarebbe sproporzionata o impraticabile.

Infine, una buona prassi consiste nel definire e documentare eventuali ulteriori ruoli e responsabilità in rapporto alle politiche, ai processi e alle disposizioni interne all'organismo – per esempio:

- se specifiche realtà aziendali propongono di condurre una DPIA, dovrebbero anche fornire input ai fini di tale DPIA e partecipare al relativo processo di validazione;
- se del caso, si raccomanda di consultare esperti indipendenti provenienti da diversi ambiti disciplinari[23] (legale, tecnologico, sicurezza, sociologico, etico, ecc.);
- ruoli e responsabilità dei responsabili di trattamento devono essere fissati in strumenti contrattuali, e la DPIA dovrebbe essere condotta con il supporto del responsabile, tenendo conto della natura del trattamento e delle informazioni di cui il responsabile dispone (art. 28, comma 3, lettera f));
- il responsabile della sicurezza dei sistemi informativi (*Chief Information Security Officer, CISO*), ove designato, nonché il RPD potrebbero proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborare con i soggetti interessati al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità del livello di rischio residuale, e definire un corpus di conoscenze specifiche del contesto operativo del titolare;

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

- ove designato, il responsabile della sicurezza dei sistemi informativi e/o l'ufficio o divisione IT dovrebbero fornire supporto al titolare e potrebbero proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza o operative.

c) Quale metodologia deve essere applicata per condurre una DPIA? Vi possono essere metodologie diverse, ma i criteri devono essere gli stessi

Il regolamento fissa le caratteristiche basilari di una DPIA all'art. 35, paragrafo 7, e nei considerando 84 e 90:

- "*una descrizione [sistematica] 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 con il presente regolamento*".

La figura seguente illustra il processo iterativo generale relativo alla conduzione di una DPIA[24]:

Il rispetto di un codice di condotta (ai sensi dell'art. 40) deve essere tenuto in considerazione (ex art. 35, paragrafo 8) nel valutare l'impatto di un trattamento. È un elemento che può risultare utile a dimostrare la scelta o l'implementazione di misure adeguate, purché il codice di condotta sia idoneo con riguardo allo specifico trattamento. Si dovrebbe tenere conto anche di eventuali certificazioni, sigilli e marchi finalizzati a dimostrare che determinati trattamenti da parte di titolari e responsabili rispettano il regolamento (art. 42) nonché di norme vincolanti d'impresa (BCR).

[24] Occorre sottolineare che il processo raffigurato ha natura iterativa; in pratica, è verisimile che ogni fase debba essere ripetuta più volte prima di completare la DPIA.

Tutti i requisiti pertinenti fissati nel regolamento offrono uno schema di ampio respiro al fine della progettazione e della conduzione di una DPIA. La realizzazione di tale DPIA sarà guidata dai requisiti fissati nel regolamento integrati da linee-direttrici di natura più concreta. L'implementazione della valutazione di impatto è, dunque, un processo scalabile, nel senso che anche un titolare di piccole dimensioni può essere in grado di progettare e attuare una DPIA assolutamente idonea ai rispettivi trattamenti.

Nel considerando 90 del regolamento sono elencati alcuni elementi della DPIA che risultano sovrapponibili a elementi ben noti di schemi esistenti per la gestione del rischio (per esempio, ISO 31000[25]). In termini di gestione del rischio, una DPIA mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche attraverso i processi di seguito indicati:

- Definizione del contesto: "*tenendo conto della natura, dell'ambito, del contesto e delle finalità del trattamento e delle fonti di rischio"*;
- Valutazione dei rischi: "*valutare la particolare probabilità e gravità del rischio elevato";*
- Gestione dei rischi: "*attenuare tale rischio*" "*assicurando la protezione dei dati personali*" e "*dimostrando la conformità al presente regolamento*".

Si osservi che la DPIA, in base al regolamento, rappresenta uno strumento finalizzato alla gestione dei rischi per i diritti degli interessati e, conseguentemente, è informata a tale prospettiva così come avviene in altri campi (per esempio, la sicurezza sociale); viceversa, la gestione del rischio così come praticata in altri ambiti (per esempio, la sicurezza delle informazioni) è focalizzata sui rischi per l'organismo stesso.

Il regolamento dà ai titolari un margine di flessibilità nello stabilire la struttura e la forma della valutazione di impatto in modo da consentirne l'inclusione nelle prassi lavorative in essere. Vi sono già oggi alcuni schemi definiti nell'Ue e a livello mondiale che tengono conto degli elementi descritti al considerando 90; tuttavia, qualunque sia la forma prescelta, la DPIA deve configurare una vera valutazione dei rischi e consentire ai titolari di adottare misure per affrontare tali rischi.

Si possono utilizzare varie metodologie (si veda l'Allegato 1, che contiene esempi di metodologie per la valutazione di impatto sulla protezione dei dati e sulla privacy) per contribuire all'attuazione dei requisiti basilari fissati nel regolamento.

Per consentire la coesistenza di approcci diversificati quali quelli sopra descritti, e contemporaneamente permettere ai titolari di rispettare le disposizioni del regolamento, sono stati individuati alcuni criteri condivisi (Allegato 2). Tali criteri illustrano i requisiti basilari previsti dal regolamento, ma lasciano un margine sufficiente per il ricorso a differenti modalità di implementazione. I criteri sono utilizzabili per dimostrare che una specifica metodologia di DPIA è conforme agli standard fissati dal regolamento. **Spetta al titolare selezionare la metodologia, che comunque deve rispettare i criteri indicati nell'Allegato 2.**

Il WP29 promuove la definizione di schemi di DPIA settoriali che possano, quindi, trarre beneficio dalle specifiche conoscenze settoriali così da consentire alla DPIA di gestire le specificità di una determinata categoria di trattamenti (per esempio: categorie particolari di dati, beni societari, impatti potenziali, minacce, misure idonee). Ciò significa che la DPIA potrà affrontare le problematiche emergenti in un determinato settore economico, ovvero legate all'impiego di una specifica tecnologia o allo svolgimento di una particolare tipologia di trattamenti.

---

[25] Processi per la gestione del rischio: comunicazione e consultazione, definizione del contesto, valutazione del rischio, gestione del rischio, monitoraggio e revisione (si vedano termini e definizioni, e l'indice contenuto nella "anteprima" visionabile della norma 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en.)

Infine, ove necessario, "*il titolare procede a un riesame per valutare se il trattamento sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento*" (art. 35, paragrafo 11).[26]

d) È obbligatorio pubblicare la DPIA? No, ma pubblicarne una sintesi può favorire un rapporto fiduciario e la si deve inviare in forma completa all'autorità di controllo in caso di consultazione preventiva ovvero su richiesta dell'autorità stessa.

La pubblicazione della DPIA non costituisce un obbligo formale ai sensi del regolamento, ed è quindi rimessa alla discrezionalità del titolare. Tuttavia, sarebbe opportuno che i titolari valutassero di rendere pubbliche almeno parti della DPIA, quali una sintesi o le conclusioni: così facendo si promuoverebbe la fiducia nelle attività di trattamento svolte da quei titolari dando prova di un approccio responsabile e trasparente. La pubblicazione della DPIA appare particolarmente indicata se il trattamento produce effetti su una parte della popolazione, il che vale soprattutto nel caso sia un'autorità pubblica a condurre la DPIA.

Non è necessario che si pubblichi la DPIA nella sua interezza, specialmente se essa contiene informazioni dettagliate rispetto ai rischi di sicurezza che investono il titolare ovvero se può rivelare segreti commerciali o informazioni di rilevanza commerciale. In casi del genere, può essere sufficiente una sintesi delle principali risultanze del processo di valutazione di impatto, o anche una semplice dichiarazione relativa all'effettuazione di una DPIA.

Inoltre, se la DPIA indica l'esistenza di un rischio residuale elevato, il titolare dovrà consultare l'autorità di controllo prima di procedere al trattamento (art. 36, paragrafo 1), e in tal caso sussiste l'obbligo di fornire la DPIA nella sua interezza all'autorità (art. 36, paragrafo 3, lettera e)). L'autorità di controllo può fornire la propria consulenza[27] senza pregiudicare segreti commerciali o rivelare vulnerabilità in termini di sicurezza, salvi i principi applicabili in ciascun Stato membro con riguardo all'accesso ai documenti pubblici.

E. Quando occorre consultare l'autorità di controllo? Se i rischi residuali sono elevati

Si è già chiarito che:

- la DPIA è necessaria quando un trattamento "*può comportare un rischio elevato per i diritti e le libertà delle persone fisiche*" (art. 35, paragrafo 1, v. III.B.a). Per esempio, si ritiene che il trattamento su larga scala di dati relativi alla salute possa comportare un rischio elevato, e quindi si rende necessaria una DPIA;
- spetta poi al titolare valutare i rischi per i diritti e le libertà degli interessati e individuare le misure[28] previste al fine di ridurre tali rischi a un livello accettabile e dimostrare l'osservanza del regolamento (art. 35, paragrafo 7, v. III.C.c.). Si pensi, per esempio, alla conservazione di dati personali su computer portatili attraverso idonee misure di sicurezza tecniche e organizzative (cifratura dell'intero hard disk, chiavi robuste di autenticazione, idonei controlli sull'accesso, backup sicuri, ecc.) unite alle modalità in essere per quanto concerne informativa, consenso, esercizio del diritto di accesso o di opposizione, ecc. .

[26] L'art. 35, paragrafo 10, esclude espressamente solo l'applicazione dei paragrafi da 1 a 7 dello stesso.
[27] La necessità di fornire una consulenza per iscritto vige soltanto se l'autorità di controllo ritiene che il trattamento prefigurato non sia conforme al regolamento, come prevede l'art. 36, paragrafo 2.
[28] Tenendo conto anche delle indicazioni, ove esistenti, del Comitato europeo per la protezione dei dati e delle autorità di controllo, nonché dello stato dell'arte e dei costi di attuazione, come prescrive l'art. 35, paragrafo 1.

Nel caso del computer portatile sopra menzionato, se il titolare ritiene che vi sia una sufficiente riduzione dei rischi e sulla base di quanto prevede l'art. 36, paragrafo 1, alla luce dei considerando 84 e 94, si può procedere al trattamento senza consultare l'autorità di controllo. Ove i rischi in precedenza identificati non possano essere gestiti dal titolare in misura sufficiente (ossia, qualora vi sia un elevato rischio residuale) il titolare è tenuto a consultare l'autorità di controllo.

Un esempio di rischio residuale elevato non accettabile [SIC] è dato dalla possibilità che l'interessato patisca conseguenze significative, o addirittura irreversibili, e non eliminabili (per esempio, in caso di accesso illecito ai dati che comporti una minaccia per la vita degli interessati, la perdita o sospensione del rapporto lavorativo, un danno finanziario), e/o dai casi in cui appare evidente che il rischio paventato si manifesterà (per esempio, a causa dell'impossibilità di ridurre il numero di soggetti in grado di accedere ai dati in ragione delle modalità di condivisione, utilizzo o distribuzione di tali dati, ovvero per l'assenza di salvaguardie contro una vulnerabilità ampiamente nota).

Qualora il titolare non sia in grado di individuare misure sufficienti a ridurre il rischio a livelli accettabili (ossia, qualora il rischio residuale continui a permanere elevato), è necessario consultare l'autorità di controllo.[29]

Inoltre, il titolare dovrà consultare l'autorità se il diritto dello Stato membro prevede l'obbligo di consultare e/o ottenere la previa autorizzazione dell'autorità stessa in rapporto a trattamenti svolti da quel titolare per l'esecuzione di compiti nell'interesse pubblico, fra cui i trattamenti connessi alla protezione sociale e alla sanità pubblica (art. 36, paragrafo 5).

Tuttavia, occorre sottolineare che, indipendentemente dall'obbligo di consultare l'autorità di controllo in base al livello di rischio residuale, vale in ogni caso l'obbligo di conservare la documentazione della DPIA e di riesaminare la DPIA periodicamente.

IV. Conclusioni e raccomandazioni

La DPIA è uno strumento che consente ai titolari di implementare sistemi di trattamento dati conformi al regolamento, e in taluni casi di trattamento la sua conduzione è obbligatoria. Si tratta di una procedura scalabile che può assumere forme diverse, tuttavia i requisiti basilari di una DPIA efficace sono fissati nel regolamento. I titolari dovrebbero guardare alla DPIA come a un'attività utile e positiva che favorisce l'osservanza dei requisiti di legge.

L'art. 24, primo paragrafo, del regolamento fissa le responsabilità essenziali del titolare del trattamento in termini di osservanza: "*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*."

[29] "*Pseudonimizzazione e cifratura di dati personali*" come pure la minimizzazione dei dati, i meccanismi di controllo, ecc. non costituiscono necessariamente misure idonee. Si tratta soltanto di esempi: l'idoneità delle misure dipende dal contesto e dai rischi specifici dei singoli trattamenti.

La DPIA è un elemento essenziale ai fini del rispetto del regolamento qualora si preveda di svolgere o si svolga un trattamento a rischio elevato. Ciò significa che i titolari dovrebbero utilizzare i criteri indicati nel presente documento per stabilire se sia o meno necessario condurre una DPIA. I titolari sono liberi, sulla base delle rispettive politiche interne, di ampliare la casistica dei trattamenti soggetti a DPIA oltre quanto richiesto dalla lettera del regolamento; in ultima analisi, così facendo si potranno accrescere la fiducia e l'affidamento degli interessati e degli altri titolari.

Se prevede di svolgere un trattamento che può presentare un rischio elevato, il titolare deve:

- selezionare una metodologia per la conduzione della DPIA (vedi esempi in Allegato 1) che soddisfi i criteri fissati nell'Allegato 2, ovvero specificare e mettere in atto una procedura sistematica di DPIA che
    - sia conforme ai criteri di cui all'Allegato 2;
    - sia parte integrante dei processi esistenti relativi alla progettazione, allo sviluppo, al cambiamento, al rischio e al riesame delle procedure operative, conformemente ai processi, ai contesti e alla cultura interni;
    - veda il coinvolgimento dei soggetti interessati e ne definisca con precisione le rispettive responsabilità (titolare, RPD/DPO, interessati o loro rappresentanti, area business, servizi tecnici, responsabili del trattamento, responsabile della sicurezza informativa, ecc.);
- fornire all'autorità di controllo competente, ove previsto, la relazione sulla DPIA svolta;
- consultare l'autorità di controllo se non è stato in grado di individuare misure sufficienti ad attenuare i rischi elevati;
- riesaminare periodicamente la DPIA e il trattamento che ne forma l'oggetto, quantomeno se intervengono variazioni del rischio posto dal trattamento in questione;
- documentare le decisioni assunte.

Allegato 1 – Esempi di schemi di DPIA attualmente esistenti nell'Ue

Il regolamento non specifica quale procedura debba essere seguita ai fini della DPIA, lasciando ai titolari la definizione di uno schema che integri le rispettive prassi e che deve, tuttavia, tenere conto delle componenti di cui all'art. 35, paragrafo 7. Può trattarsi di uno schema di DPIA sviluppato in rapporto alle specifiche esigenze del titolare, ovvero utilizzabile da un intero settore produttivo. Nel prosieguo si fornisce un elenco (non esaustivo) di schemi di DPIA già pubblicati ed elaborati da autorità per la protezione dei dati nell'Ue nonché su base settoriale:

Esempi di schemi di DPIA generali:

- DE: Standard Data Protection Model, V.1.0 – Trial version, 2016[30].
  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 schemi di DPIA settoriali:

- Privacy and Data Protection Impact Assessment Framework for RFID Applications.[31]
  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[32]
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

---

[30] Approvato all'unanimità (con l'astensione del Land Baviera) dalla 92ma Conferenza delle autorità indipendenti per la protezione dei dati della Federazione e dei Länder a Kühlungsborn, 9-10 novembre 2016.

[31] Si veda anche:
- Raccomandazione della Commissione del 12 maggio 2009 sull'attuazione dei principi di privacy e protezione dati nelle applicazioni supportate dall'identificazione attraverso radiofrequenze.
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Parere 9/2011 sulla proposta rivisitata, presentata dai produttori, di uno schema di valutazione di impatto sulla privacy e la protezione dei dati ai fini delle applicazioni RFID
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf

[32] Si veda anche il Parere 7/2013 concernente il modello di valutazione di impatto sulla protezione dei dati per i sistemi basati sulle griglie intelligenti e i contatori intelligenti, predisposto dall'Expert Group 2 della Task Force della Commissione europea sulle griglie intelligenti.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

Inoltre, uno standard internazionale (ISO/IEC 29134) fornirà linee direttrici in merito alle metodologie utilizzabili per la conduzione di una DPIA.[33]

[33] ISO/IEC 29134 (progetto) *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO).

Allegato 2 – Criteri riferiti a una DPIA accettabile

Il WP29 propone i seguenti criteri utilizzabili dai titolari di trattamento per stabilire se una DPIA, o una metodologia specifica di DPIA, comprenda un numero di elementi sufficienti a garantire il rispetto delle disposizioni del regolamento:

- descrizione sistematica del trattamento (art. 35, paragrafo 7, lettera a)):
  - si tiene conto della natura, dell'ambito, del contesto e delle finalità del trattamento (considerando 90);
  - sono indicati i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi;
  - si dà una descrizione funzionale del trattamento;
  - si specificano gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
  - si tiene conto dell'osservanza di codici di condotta approvati (art. 35, paragrafo 8);
- valutazione di necessità e proporzionalità del trattamento (art. 35, paragrafo 7, lettera b)):
  - si definiscono le misure previste per rispettare il regolamento (art. 35, paragrafo 7, lettera d) e considerando 90) tenendo conto di quanto segue:
    - misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
      - finalità specifiche, esplicite e legittime (art. 5(1), lettera b));
      - liceità del trattamento (art. 6);
      - dati adeguati, pertinenti e limitati a quanto necessario (art. 5(1)c));
      - periodo limitato di conservazione (art. 5(1), lettera e));
    - misure che contribuiscono ai diritti degli interessati:
      - informazioni fornite agli interessati (artt. 12, 13, 14);
      - diritto di accesso e portabilità dei dati (artt. 15 e 20);
      - diritto di rettifica e cancellazione (artt. 16, 17, 19); diritto di opposizione e limitazione del trattamento (artt. 18,19, 21);
      - rapporti con responsabili del trattamento (art. 28);
      - garanzie per i trasferimenti internazionali di dati (Capo V);
      - consultazione preventiva (art. 36);
- gestione dei rischi per i diritti e le libertà degli interessati (art. 35, paragrafo 7, lettera c):
  - si determinano l'origine, la natura, la particolarità e la gravità dei rischi (v. considerando 84) o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati:
    - si tiene conto delle fonti di rischio (considerando 90);
    - si identificano gli impatti potenziali sui diritti e le libertà degli interessati in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilità dei dati;
    - si identificano le minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilità dei dati;
    - si stimano probabilità e gravità (considerando 90);
  - si stabiliscono le misure previste per gestire i rischi di cui sopra (art. 35, paragrafo 7, lettera d) e considerando 90);
- coinvolgimento dei soggetti interessati:
  - si chiede consulenza al RPD/DPO (art. 35, paragrafo 2);
  - si sentono gli interessati o i loro rappresentanti (art. 35, paragrafo 9), se del caso.