Valutazione d'impatto sulla protezione dei dati (DPIA): obblighi e procedure per gli enti pubblici

A domanda risponde Prof. Avv. Michele IASELLI

31 ottobre 2024 - dalle ore 9.30 alle 10.30

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione
degli Enti Locali
Email info@dpoinrete.it
Numero Verde 800.16.56.54
Web: www.dpoinrete.it
www.asmel.eu

Previsione normativa

L’art. 35 del Regolamento parla di **valutazione d’impatto sulla protezione dei dati** che deve essere effettuata dal titolare del trattamento quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l’oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La valutazione contiene almeno:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, se del caso, 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.

Inoltre la valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei seguenti casi:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata sul trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono allo stesso modo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c) la sorveglianza sistematica di una zona accessibile al pubblico su larga scala.

Come già accaduto in Italia, l'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati. La stessa Autorità comunica tali elenchi al Comitato europeo per la protezione dei dati.
L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. Anche tali elenchi sono comunicati dall'Autorità al Comitato europeo per la protezione dei dati.

Prima di adottare tali elenchi l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 del Regolamento (che richiede una operazione delle Autorità di controllo per un’applicazione coerente del Regolamento) se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al controllo 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.
Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili si tiene debito conto, anche, del rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

Linee guida Garanti Europei

Il 4 aprile 2017 con primo emendamento avvenuto il 4 ottobre 2017), in materia, sono state pubblicate delle linee guida dei Garanti europei che hanno cercato di fornire utili chiarimenti in una materia sicuramente molto complessa.

In realtà nelle linee guida viene precisato che 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.

Quando si parla di 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 GDPR, 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.

Oggetto della DPIA

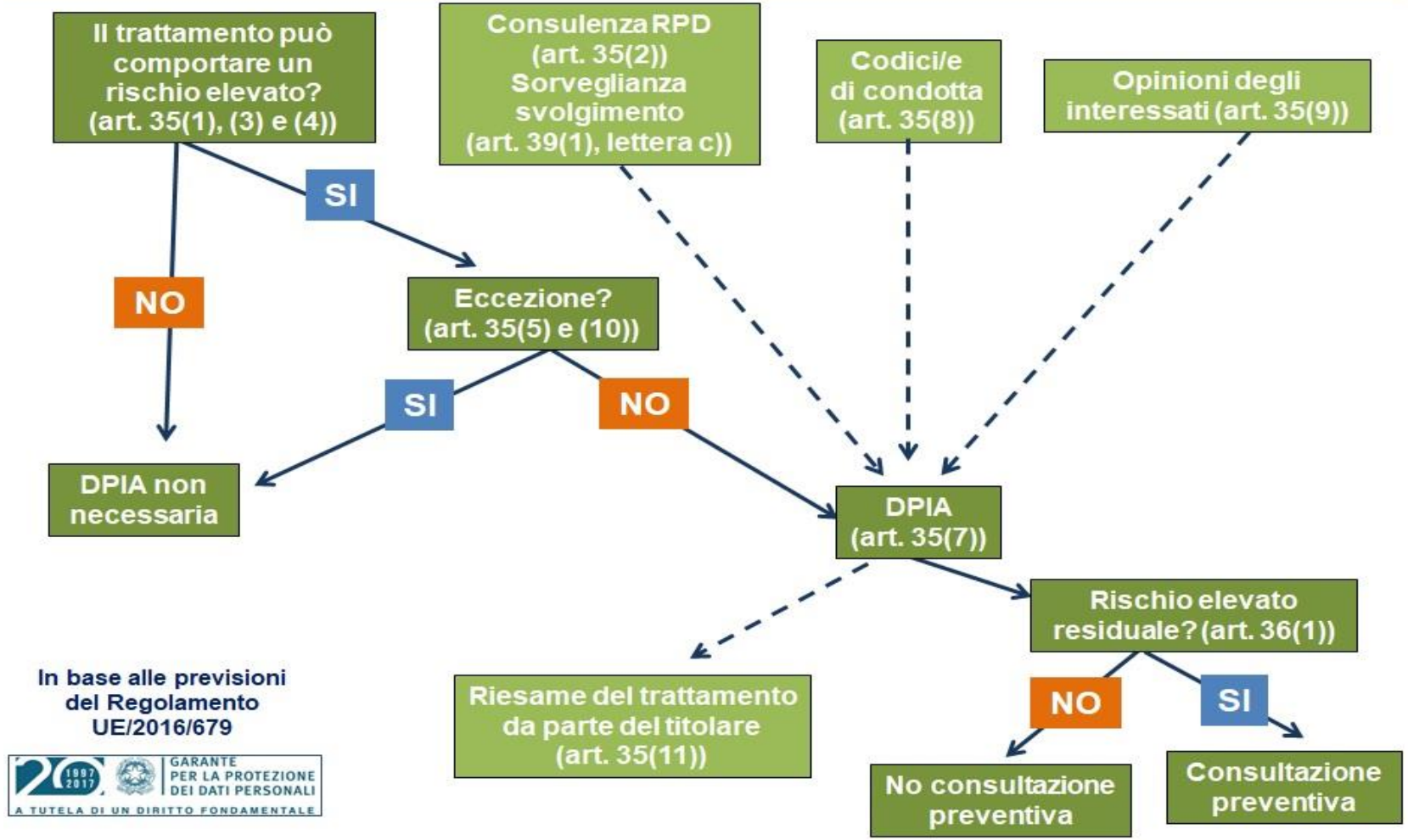
Nelle linee guida viene innanzitutto precisato che una singola DPIA per quanto può riguardare una sola operazione di trattamento dei dati potrebbe essere utilizzata per valutare molteplici operazioni di trattamento che sono simili in termini di rischi presentati, purché adeguatamente considerate la specifica natura, portata, contesto e finalità del trattamento.

Si può fare riferimento, quindi, a tecnologie simili utilizzate per raccogliere lo stesso tipo di dati per le medesime finalità. Ad esempio, un gruppo di autorità municipali in cui ciascuno predisponga un simile sistema TVCC potrebbe effettuare un' unica DPIA che copra l'elaborazione di questi titolari separati, o un operatore ferroviario (singolo titolare) potrebbe 'coprire' la videosorveglianza in tutte le sue stazioni con una DPIA.

Una DPIA può anche essere utile per valutare l'impatto di protezione di dati di un prodotto tecnologico, per esempio un componente hardware o software, qualora ciò sia suscettibile ad essere utilizzato da altri titolari per effettuare diversi trattamenti.
Naturalmente, il titolare del trattamento che distribuisce il prodotto, rimane obbligato a svolgere la propria DPIA per quanto riguarda l'attuazione specifica, ma questo può essere messo al corrente della DPIA preparata dal fornitore del prodotto, se del caso.

dpo in rete

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



In base alle previsioni del Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE

Esempi di lavorazione	Possibili criteri	DPIA richiesta?
Il trattamento dei dati genetici e di salute dei pazienti in un ospedale (sistema informativo dell'ospedale).	I dati sensibili Dati relativi interessati vulnerabili	Si
L'uso di un sistema di telecamere per monitorare il comportamento di guida in autostrada. Il titolare prevede di utilizzare un sistema di analisi video intelligente per individuare autoveicoli e riconoscere automaticamente le targhe.	Il monitoraggio sistematico L'uso innovativo o l'applicazione di soluzioni tecnologiche o organizzative	
Una società che monitora le attività dei suoi dipendenti inclusa la loro postazione di lavoro, attività internet, ecc	Il monitoraggio sistematico I dati relativi interessati vulnerabili	
La raccolta di dati dai profili social usate da compagnie private per generare profili per database di contatti	Valutazione o assegnazione di un punteggio I dati trattati su larga scala	
Una rivista online utilizza una mailing list per inviare un sommario giornaliero generico ai suoi abbonati.	Nessuno	Non necessariamente
Un sito di e-commerce visualizza annunci pubblicitari di auto d'epoca includendo una limitata profilazione ispirata al passato comportamento d'acquisto su alcune parti del proprio sito Web.	Valutazione o assegnazione di un punteggio, ma non sistematica o estesa	

Metodologia della DPIA

Le linee guida suggeriscono, inoltre, diverse metodologie per effettuare una DPIA anche se i criteri naturalmente devono essere comuni.
In merito è stata predisposta una specifica norma internazionale ISO/IEC 29134 dal titolo "*Privacy Impact Assessment – Methodology*" che propone: un processo molto articolato in 12 passi, a cui ne vanno aggiunti 2 di riesame periodico o ad hoc e di attuazione degli eventuali cambiamenti necessari; un indice in 6 punti per il rapporto di valutazione ed un esempio per la stima degli impatti.

Nel considerando 90 del GDPR 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). 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 regolamento*".

Analisi dei rischi

Una valutazione approfondita dei rischi è possibile solo se si evidenziano gli elementi che caratterizzano il trattamento dei dati, per cui il titolare del trattamento dovrà descrivere:

- su quali processi aziendali si distribuiscono le componenti del trattamento previste;
- quali informazioni sono utilizzate nelle singole fasi;
- quali asset (es. hardware, software, reti, persone, canali di trasmissione, documenti cartacei) sostengono il trattamento nelle singole fasi;
- a cosa servono i dati, ovvero per quale finalità;
- da chi sono ottenute le informazioni, a chi sono comunicate;
- chi ne deve avere accesso.

Questa fase della procedura di DPIA può essere supportata da fonti informative già disponibili all'interno dell'organizzazione del Titolare per descrivere come i dati saranno utilizzati (es. un diagramma che riporti i flussi informativi tra i vari soggetti o sistemi o processi, la sequenza prevista delle operazioni di gestione dei dati, rapporti sull'uso delle informazioni, mappe informative, registri di asset informativi), a partire da quanto già raccolto in fase di Valutazione Preliminare.

Identificazione delle diverse categorie di rischi

In questa fase occorre valutare gli aspetti che espongono il trattamento in esame a rischi di protezione e a rischi di sicurezza (informatica o fisica) dei dati personali. Più correttamente, o quanto meno in relazione a definizioni e concetti derivanti da standard internazionali in materia di *Risk Management,* il Regolamento con il termine *Rischi* si riferisce alle c.d. *minacce,* ovvero le categorie di eventi che possono determinare un effetto negativo sull'Interessato (materiale o immateriale, vedere Considerando 83), ed in altri casi alle possibili *conseguenze* o *tipologie di violazioni* sui trattamenti.

Una corretta analisi dei rischi dovrebbe, quindi, tener conto:

- la tipologia dei dati trattati, la loro appetibilità, nonché la loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- i comportamenti degli operatori, gli eventi relativi agli strumenti utilizzati per il trattamento dei dati, gli eventi relativi al contesto.

Comportamento degli operatori

Rischi	Si/No	gravità
Sottrazione di credenziali di autenticazione	Si	Bassa
Carenza di consapevolezza, disattenzione o incuria	Si	Bassa
Comportamenti sleali o fraudolenti	Si	Bassa
Errore materiale	Si	Bassa
Altro evento	Si	Bassa

Eventi relativi agli strumenti

Rischi	Si/No	gravità
Azione di virus informatici o di programmi suscettibili di recare danno	Si	Bassa
Spamming o tecniche di sabotaggio	Si	Bassa
Malfunzionamento, indisponibilità o degrado degli strumenti	Si	Media
Accessi esterni non autorizzati	Si	Media
Intercettazioni di informazioni in rete	Si	Media
Altro evento	No	////////

Eventi relativi al contesto

Rischi	Si/No	gravità
Accessi non autorizzati a locali/aree ad accesso ristretto	Si	Media
Sottrazione di strumenti contenenti dati	Si	Bassa
Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, ecc.) nonché dolosi, accidentali o dovuti ad incuria	Si	Bassa
Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	Si	Bassa
Errori umani nella gestione della sicurezza fisica	Si	Bassa
Altro evento	No	////////

Quesiti
Quanti dati personali potrebbero essere divulgati, modificati o resi indisponibili?
Chi sono gli individui i cui dati potrebbero essere divulgati, modificati o resi indisponibili? Staff (dipendenti, collaboratori), dati relativi a propri clienti o fornitori, o dati relativi ai clienti dei propri servizi?
Quanto sono sensibili i dati che potrebbero essere divulgati, modificati o resi indisponibili? Sono incluse categorie speciali di dati, dati finanziari, informazioni pubbliche, ... ?
Che cosa potrebbero rilevare di un individuo a una terza parte se i dati dello stesso fossero divulgati, manomessi o resi indisponibili?
Che conseguenze potrebbero avere questi individui? Ci potrebbero essere rischi alla salute o alla reputazione, perdite finanziarie o una combinazione di questi o ad altri aspetti della propria vita? La violazione potrebbe comportare un furto di identità o una frode, danni fisici, disturbi psicologici, umiliazione o un danno reputazionale?
Ci potrebbero essere conseguenze più ampie quali un rischio alla salute pubblica, o la perdita di fiducia in un servizio offerto dall'organizzazione?

SCENARI RID

R – perdita di Riservatezza: i dati personali sono divulgati ad individui, organizzazioni, enti non autorizzati;

I – Violazione dell'Integrità: i dati personali sono incompleti o non corretti o modificati senza le opportune autorizzazioni;

D – Perdita della disponibilità: i dati personali non sono accessibili o utilizzabili quando necessario.

Il WP29 incoraggia, inoltre, lo sviluppo di quadri DPIA settoriali. Questo perché essi possono attingere a conoscenze specifiche di settore, il che significa che la DPIA si può indirizzare alle specifiche di un particolare tipo di operazione di trattamento (es.: particolari tipi di dati, beni aziendali, le potenziali ripercussioni, minacce, misure). In questo modo la DPIA può risolvere i problemi che sorgono in un particolare settore economico, o se si utilizzano particolari tecnologie o si effettuano particolari tipi di operazioni di trattamento.

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.

I trattamenti necessariamente soggetti alla DPIA

Con il provvedimento n. 467 dell'11 ottobre 2018 pubblicato sulla G.U. n. 269 del 19 novembre 2018 il Garante per la protezione dei dati personali ha previsto, ai sensi dell'art. 35 comma 4 del Regolamento UE n. 2016/679, l'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati.

Come precisato dalla stessa Autorità nel proprio provvedimento, non si tratta di un'iniziativa autonoma, ma nel rispetto di quanto previsto dal Regolamento e, quindi, dallo stesso principio di coerenza, tale elenco è stato condiviso in ambito comunitario e comunicato al Comitato Europeo per la protezione dei dati, che ha espresso, in merito, specifico parere recepito dall'Autorità.

Analizzando, nello specifico, i trattamenti previsti dal Garante, peraltro non esaustivi, si nota come vengono ripresi e precisati quei trattamenti già indicati dai Garanti europei (WP29) nelle loro linee guida e del resto non poteva essere diversamente in quanto una base condivisa a livello comunitario si rendeva necessaria.

Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato".

Trattamenti automatizzati finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi).

Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

Trattamenti effettuati nell’ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell’attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).

Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev.01.

Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.

Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).

Trattamenti di categorie particolari di dati ai sensi dell’art. 9 oppure di dati relativi a condanne penali e a reati di cui all’art. 10 interconnessi con altri dati personali raccolti per finalità diverse.

Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell’attività di trattamento.

Quando una DPIA non è necessaria?

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

1. se il trattamento non "*può comportare un rischio elevato per i diritti e le libertà di persone fisiche" (art. 35, paragrafo 1).*

2. 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).

3. 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.

4. 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), tranne ove uno Stato membro abbia previsto la necessità di condurre una DPIA per i trattamenti pregressi.

5. 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.

Quando si effettua una DPIA?

La DPIA dovrebbe essere condotta “prima di procedere al trattamento” (art. 35, paragrafo 1, e art. 35, paragrafo 10; considerando 80 e 93). Tale impostazione è coerente con i principi della privacy by design e by default (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.

Lo svolgimento della DPIA è un processo continuativo e non un’attività *una tantum.*

Chi è tenuto a condurre la DPIA?

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)).

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).

Quando occorre consultare il Garante?

Spetta al titolare valutare i rischi per i diritti e le libertà degli interessati e individuare le misure previste al fine di ridurre tali rischi a un livello accettabile e dimostrare l'osservanza del regolamento (art. 35, paragrafo 7).
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. .

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.

Consultazione preventiva

L’art. 36 del GDPR prevede la c.d. consultazione preventiva quando il titolare del trattamento, prima di procedere al trattamento dei dati personali, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

Se l'Autorità di controllo ritiene che il trattamento previsto non sia conforme al Regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, entro un periodo massimo di otto settimane dalla richiesta di consultazione, fornisce una consulenza per iscritto al titolare del trattamento dei dati, e ove applicabile al responsabile del trattamento. Questo periodo può essere prorogato di ulteriori sei settimane, tenendo conto della complessità del trattamento previsto. Qualora si applichi la proroga, il titolare del trattamento e, ove applicabile, il responsabile del trattamento ne sono informati, incluso dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Buone pratiche e strumenti utili per la DPIA

- Strumenti utili
- Buone pratiche
- Risorse e modelli
- Errori comuni e come evitarli