# Quando procedere ad una DPIA ex art. 35 GDPR: la “prevalutazione d’impatto”

**Author :** Mauro Formato

**Date :** 24 luglio 2018

Tra le novità introdotte dalla nuova disciplina europea in materia di protezione dei dati (Reg. UE 2016/679 – G.D.P.R.) un posto di rilievo spetta sicuramente alla Valutazione d’impatto sulla protezione dei dati (anche detta DPIA – Data Protection Impact Assessment), disciplinata dall’art. 35 del Regolamento [1].

Tale norma prevede che la DPIA contenga almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l’interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- 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 regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Obiettivo del presente intervento non sarà tuttavia analizzare ed individuare prontamente la corretta metodologia da seguire per redigere una DPIA, bensì provare a chiarire qualche zona d’ombra creatasi intorno alla stessa e, in particolare, fornire alcuni suggerimenti utili per identificare i casi in cui diviene necessario effettuare una Valutazione d’impatto.

**Preliminarmente, cos’è la DPIA?**

Una procedura intesa a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire ad identificare e gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

Una DPIA consente quindi al Titolare di analizzare sistematicamente e approfonditamente come

un nuovo trattamento, una nuova tecnologia, o un nuovo progetto (ovvero una modifica sostanziale ad un trattamento già in corso o l'impiego per finalità o con metodologie differenti di tecnologie già esistenti) impatteranno sui diritti e le libertà degli interessati e individuare, con un approccio *privacy by design & by default*, quali misure implementare per la tutela di quest'ultimi.

L'art. 35 Reg. UE 2016/679 prevede che la DPIA sia obbligatoria in caso di trattamenti che per natura, oggetto, contesto e finalità, possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Identificare i casi che ricadono nello scenario prima richiamato, però, non sempre costituisce operazione semplice ed immediata, ma necessita di una fase preliminare - **definibile prevalutazione d'impatto** - nella quale il Titolare, raccolte le informazioni essenziali sul trattamento che intende introdurre o modificare, valuterà l'opportunità e/o la necessità di procedere o meno ad una DPIA.

Il GDPR infatti, proseguendo nella campagna di sensibilizzazione e responsabilizzazione del Titolare, non elenca tassativamente i casi nei quali è obbligatorio procedere ad una DPIA, ma si limita ad elencare tre ipotesi nelle quali essa è richiesta, in particolare:

a. quando il trattamento comporta 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;
b. nel caso di 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;
c. qualora il trattamento abbia ad oggetto la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;

Il Regolamento Europeo pertanto affida al solo Titolare, coadiuvato dal D.P.O (qualora designato), il compito di valutare se il trattamento progettato rientri o meno tra i casi per i quali la DPIA è obbligatoria.

Al fine di agevolare il Titolare nel compiere tale ardua operazione, l'Article 29 Working Party (oggi European Data Protection Board) ha emanato delle Linee Guida (WP 248) [2] contenenti nove criteri in presenza dei quali si può desumere che il trattamento presenti "*un rischio elevato per i diritti e le libertà delle persone fisiche*":

I. valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "*aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato*";
II. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo

significativamente su dette persone fisiche;

III. monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
IV. dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10;
V. trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:
    - il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
    - il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
    - la durata, ovvero la persistenza, dell'attività di trattamento;
    - la portata geografica dell'attività di trattamento;
VI. creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;
VII. dati relativi a interessati vulnerabili: il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti;
VIII. uso innovativo o applicazione di nuove soluzioni tecnologiche o organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, etc.;
IX. quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto". Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto.

In particolare, il WP ha delineato la seguente regola di condotta: **in presenza di un trattamento che soddisfi almeno due dei nove criteri la DPIA è necessaria**.

Per completezza, si ritiene opportuno precisare che, mutuando le parole utilizzate dal WP, “*un Titolare del trattamento può ritenere, anche se un trattamento soddisfa soltanto uno di questi criteri, che possa comunque richiedere una valutazione d'impatto sulla protezione dei dati, in quanto potrebbe presentare dei rischi elevati per i diritti e le libertà degli interessati*”.

Occorre infatti chiarire che, anche qualora non prevista come obbligatoria, la DPIA può essere valutata come importante strumento di accountability per dimostrare la conformità del Titolare al G.D.P.R. oltre che utile procedura per identificare concretamente le misure di sicurezza idonee ai trattamenti in atto ed ai loro relativi rischi.

Un ulteriore supporto operativo, utile al Titolare nel valutare l'opportunità di procedere o meno ad una DPIA, è fornito dall'Autorità Garante Inglese (Information Commissioner's Office) che, superando per quanto riguarda il livello di dettaglio quanto delineato dal WP, ha individuato dieci casistiche (alcune delle quali, ad onor del vero, rientranti nei nove criteri prima definiti) in presenza delle quali la DPIA sarà obbligatoria [3]:

1. **Nuove tecnologie:** il trattamento comporta l'uso di nuove tecnologie o applicazioni innovative di tecnologie esistenti (comprese le Intelligenze Artificiali).
2. **Diniego di un servizio:** decisioni concernenti l'accesso di un individuo ad un prodotto, servizio, opportunità o benefit basate su processi decisionali automatizzati o che coinvolgono il trattamento di speciali categorie di dati.
3. **Monitoraggio su larga scala:** qualsiasi monitoraggio di individui su larga scala [N.d.R. - il concetto di larga scala non viene definito esplicitamente dal G.D.P.R., tuttavia qualche indicazione in merito è desumibile dalle stesse linee guida pubblicate dall'ICO che riconduce a tale concetto, ad esempio, il trattamento dei dati dei pazienti di un ospedale, il monitoraggio dei cittadini che usano il sistema di trasporto pubblico, il trattamento dei dati degli utenti effettuato da un fornitore di linea internet o telefonica; allo stesso modo, l'Autorità Inglese, ha esplicitamente escluso dal concetto di larga scala i trattamenti concernenti dati dei propri pazienti o clienti effettuati da singoli professionisti, palesando un parere del tutto concorde a quello espresso sul punto dall'Autorità italiana]. [3]
4. **Dati biometrici:** qualsiasi trattamento di dati biometrici.
5. **Dati genetici:** qualsiasi trattamento di dati genetici, diversi da quelli trattati da singoli medici di famiglia o altri professionisti in campo sanitario per fornire cure ai singoli individui.
6. **Combinazione di dati:** combinazione, comparazione o abbinamento di dati personali ottenuti da fonti diverse.
7. **"Trattamenti invisibili":** trattamenti di dati personali che non sono stati ottenuti direttamente dall'interessato al verificarsi di circostanze nelle quali il Titolare ritiene che la compliance con l'art. 14 G.D.P.R. sia impossibile o comporti un costo sproporzionato [N.d.R. - l'art 14 G.D.P.R. impone al Titolare l'obbligo di fornire l'informativa sul trattamento dei dati personali all'interessato anche qualora gli stessi siano raccolti non presso gli interessati ma da altra fonte; un'esemplificazione di quando ciò possa avvenire è data dallo stesso considerando 62 nel quale è possibile leggere " *quest'ultima eventualità potrebbe verificarsi, ad esempio, nei trattamenti eseguiti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi si può tener conto del numero di interessati, dell'antichità dei dati e di eventuali garanzie adeguate in essere*"]
8. **Tracciamento:** trattamenti che comportano il tener traccia della geolocalizzazione di un interessato o del suo comportamento, incluso e non limitato all'ambiente online.
9. ***Targeting* di bambini o di altre categorie vulnerabili di individui:** l'uso di dati personali di bambini o di altre categorie vulnerabili di individui per finalità di marketing, profilazione oppure altri trattamenti decisionali automatizzati, ovvero nel caso si servizi online offerti direttamente ai bambini.
10. **Pericolo di danni fisici:** quando la natura del trattamento è tale che un data breach può mettere a repentaglio la salute (fisica) o la sicurezza degli individui.

Un primo approccio alla "***prevalutazione d'impatto***" potrebbe pertanto consistere nel trasferire i criteri e le casistiche sin qui richiamate in una checklist, stabilire il numero di match in presenza del quale la DPIA è da ritenersi obbligatoria (uno - sposando le indicazioni fornite dall'ICO - due - sposando le indicazioni fornite dal W.P.) e confrontare il trattamento progettato con la detta checklist in modo da consegnare nelle mani del Titolare uno strumento, seppur sicuramente migliorabile ed integrabile, che possa fungere da rudimentale guida nell'arduo compito di dare attuazione al par. 1 dell'art. 35 G.D.P.R.

Tutto ciò in attesa che il Garante Privacy Italiano, dando attuazione a quanto disposto dall'art. 35 par. 4 G.D.P.R., pubblichi "l'*elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati*" - che sicuramente costituirà un validissimo punto di partenza per la concreta applicazione della norma richiamata.

Anche in questo caso però, un'idea su ciò che avverrà a seguito della detta pubblicazione viene fornita dall'Autorità Garante Inglese che, anticipando sul tempo l'Autorità Italiana, ha già individuato una lista di trattamenti considerati come ad alto rischio (Examples of processing "*likely to result in high risk*") [4]

Trattasi di un elenco (non definitivo e soggetto a modifiche, come sarà d'altronde quello che verrà emanato dal Garante Italiano) di ben sessantaquattro trattamenti, raggruppati nelle dieci casistiche analizzate in precedenza, per i quali il Titolare dovrà necessariamente procedere ad una DPIA.

Pur facendo a meno di un'elencazione puntuale di tali trattamenti ad alto rischio (per la quale si rimanda al link n.4 presente nella sitografia), appare tuttavia opportuno richiamare l'attenzione del lettore su alcuni trattamenti che assumono particolare rilevanza nella quotidianità per gran parte dei Titolari, quali, ad esempio, quelli attinenti il mondo del lavoro.

A parere dell'ICO infatti, qualsiasi Titolare che voglia introdurre nell'ambiente di lavoro (incluso il c.d. *remote working*) un sistema in grado di tracciare o monitorare la posizione, il rendimento, o altri dati relativi ai propri dipendenti - si pensi, ad esempio, a sistemi di valutazione continua delle prestazioni dei singoli dipendenti, ovvero a sistemi elettronici di monitoraggio continuo della posizione dei lavoratori tramite GPS - non potrà esimersi dall'effettuare una DPIA, pena la violazione dell'art.35 G.D.P.R. con conseguente possibilità di pesanti sanzioni amministrative pecuniarie (si ricorda infatti che la non conformità all'art. 35 può essere punita con una sanzione pari sino fino a **€10.000.000,00** ovvero, per le imprese, fino al **2% del fatturato mondiale** totale annuo dell'esercizio precedente se tale importo risulta essere superiore a €10.000.000,00).

Ulteriore ambito meritevole di particolare attenzione per tutti i Titolari che esercitino o promuovano la propria attività commerciale attraverso il web può essere individuato nelle attività rientranti nei cosiddetti "*invisible processing*".

Ogni titolare che desideri avvalersi di strumenti quali il marketing diretto attraverso il canale web, il riutilizzo di dati pubblici resi disponibili, l'online advertising ovvero il tracciamento degli utenti online tramite servizi offerti da terze parti, dovrà infatti necessariamente procedere ad una

DPIA al fine di dimostrare la conformità con la normativa vigente in materia di dati personali.

Appare pertanto evidente come individuare correttamente quando e come effettuare una Valutazione d'impatto costituisca un'operazione imprescindibile per il Titolare che voglia porsi al riparo da possibili sanzioni, oltre che uno strumento per monitorare costantemente e contribuire a proteggere efficacemente i dati trattati nell'ambito della propria struttura aziendale.

A tal fine, l'elencazione fornita dall'ICO potrebbe costituire una valida linea guida nelle mani del Titolare, un "database" al quale fare *medio tempore* riferimento nell'attesa di un similare pronunciamento ad opera dell'Autorità Garante italiana.

## SITOGRAFIA:


- [1] https://www.garanteprivacy.it/regolamentoue
- [2] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
- [3] https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/data-protection-impact-assessments-dpias-guidance
- [4] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/


A cura di: **Mauro Formato**