Guida per lo svolgimento della valutazione d’impatto sulla protezione dei dati (DPIA) - Parte I

Author : Marco Carbonelli

Date : 29 Giugno 2020

Il presente è il primo di una serie di **cinque articoli** che saranno pubblicati nelle prossime settimane.

Sommario

Dopo aver introdotto gli elementi indispensabili per comprendere quale sia lo scopo della **valutazione d’impatto sulla protezione dei dati**, come prospettata dalla normativa vigente nell’ambito della *privacy*, viene presentata una Guida utile per poter svolgere in modo strutturato la DPIA (*Data Protection Impact Assessment*).

Nella Guida si dettagliano in modo puntuale le varie fasi necessarie per arrivare a una valutazione ragionata e specifica del rischio dei processi legati al trattamento di dati personali. La Guida proposta può risultare utilmente applicata nelle strutture della Pubblica Amministrazione centrale e locale che, spesso, svolgono con personale proprio le azioni di analisi dei processi e di valutazione dell’impatto.
Viene anche proposto un metodo speditivo semplificato per la **quantificazione del rischio** del processo analizzato. A completamento dell’analisi vengono fornite delle schede operative di riferimento per svolgere in modo guidato e, al contempo, adeguatamente rigoroso tutte le fasi della valutazione d’impatto sulla protezione dei dati.

1. La finalità della Guida sulla DPIA

1.1. Finalità

Questo articolo si propone di fornire una **Guida** ai **Titolari di trattamenti di dati personali** e ai loro collaboratori, al fine di svolgere la **valutazione d'impatto sulla protezione dei dati** (*Data Protection Impact Assessment* = **DPIA**) richiesta dal Regolamento UE 679/2016 (GDPR).

Nel seguito del lavoro indicheremo con la sola parola **Regolamento** il riferimento al Regolamento UE 679/2016 (GDPR) e utilizzeremo **Art.x** per indicare l’articolo *x* di tale Regolamento.

La DPIA costituisce il momento più **complesso** nel ciclo di protezione dei dati personali perché, proprio con la DPIA, si valutano i rischi che possono essere indotti da un cattivo o non sufficientemente protetto trattamento dei dati.

Va subito precisato che **non esiste un metodo univoco per svolgere la DPIA**; ma le indicazioni fornite dal Regolamento, l'esperienza del Data Protection Working Party UE - noto come WP Art.29 a livello Europeo - ereditata dall'**EDPB** (European Data Protection Board) - le indicazioni del **Garante nazionale** per la protezione dei dati personali e delle principali **Autorità di Controllo Nazionali in Europa** (in particolare in Gran Bretagna con l'Information Commissioner's Officer – **ICO** - e in Francia con il **CNIL** - Commission Nationale de l'Informatique et des Libertés) consentono di individuare possibili percorsi preferenziali per condurre la valutazione DPIA.

Nel seguito di questa Guida viene delineato un percorso che si ritiene **efficace ed efficiente**, sia nella PA sia in ambiente privato, per svolgere questa valutazione. Tale percorso recepisce, oltre che i dettami del Regolamento, le indicazioni del Garante nazionale al momento disponibili [Gar1], integrandole con i suggerimenti forniti dal WP Art.29 a livello europeo [UE1] e con l'esperienza internazionale proposta dall'ICO UK [ICO1] e, per alcuni ambiti, dal CNIL francese [CNI1]. Il **percorso** è strutturato su otto **fasi** puntuali che, in **assenza di altri modelli** di riferimento preferiti dal Titolare, **possono costituire un riferimento adeguato** per lo svolgimento della DPIA.

Entrando nello specifico, nel Cap.2 si presentano le informazioni di base indispensabili per poter iniziare il lavoro di valutazione, rispondendo a **dodici domande propedeutiche** alle analisi del percorso successivo.

Nel Cap.3 si analizza in dettaglio la fase iniziale della DPIA: questa coincide con un'**analisi preliminare** che conduce alla decisione del Titolare a riguardo della necessità, o meno, di svolgere una DPIA completa per il trattamento considerato.

Nel Cap.4, una volta deciso che è necessaria per un trattamento una DPIA completa, si entra nel vivo della valutazione e vengono descritte in dettaglio le azioni da svolgere e come costruire, con delle schede proposte nelle Appendici del documento, la relazione tecnica di valutazione che accompagna ogni DPIA. In questo capitolo viene anche proposto il **metodo per la valutazione del rischio**, un metodo speditivo semplificato e progettato *ad hoc*, tenendo in considerazione le esperienze del Regno Unito e della Francia in questo ambito.

2. L'essenziale da conoscere prima di affrontare una DPIA

In questo capitolo vengono date 12 dettagliate risposte a 12 quesiti che si pongono in modo naturale quando si affronta lo svolgimento di una DPIA.

2.1 Cosa è una DPIA?

L'articolo 35 del Regolamento introduce il concetto di **valutazione d'impatto sulla protezione dei dati** (Data Protection Impact Assessment = **DPIA**) e stabilisce che "*quando un tipo di*

trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".

In altre parole, quando un trattamento può comportare un **rischio elevato per i diritti e le libertà delle persone** interessate - a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono trattati, ad esempio, dati di *categorie particolari* (Art.9), o anche per una combinazione di questi e altri fattori-, il Regolamento **obbliga** i Titolari a **svolgere una valutazione di impatto prima** di darvi **inizio**, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il **rischio residuo per i diritti e le libertà degli interessati resti elevato**.

In estrema sintesi, la DPIA è un processo di analisi finalizzato a supportare il Titolare di un trattamento al fine di **identificare** e **minimizzare** i rischi relativi alla protezione dei dati.

La finalità della DPIA non è quella di **eliminare tutti i rischi**, ma quella di **aiutare** il Titolare a **minimizzarli**, determinando se il livello di rischio residuo **risulti accettabile** o meno.

Riferimenti al Regolamento per approfondimenti

Art.35 (punto1) e Considerando n. 84 e 90

2.2. Esiste un unico metodo per svolgere la DPIA?

Non esiste un unico metodo o modello di riferimento per lo svolgimento della DPIA.

Il Regolamento stabilisce all'Art.35 punto 7 gli elementi di analisi **minimale** che debbono essere considerati nella valutazione. Tali elementi sono qui di seguito riportati.

Regolamento - Art.35 punto 7

La valutazione (DPIA) contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

A partire dal cap.3 di questa Guida viene illustrato un **percorso logico** strutturato su otto **Fasi** che, in **assenza di altri modelli** di riferimento preferiti dal Titolare, può costituire un punto di partenza **adeguato** e **comune** per lo svolgimento della DPIA.

2.3 Chi ha la responsabilità di svolgere la DPIA?

La responsabilità della DPIA spetta al **Titolare** del trattamento (in inglese *Data Controller*), anche se la conduzione materiale della valutazione di impatto può essere affidata, in linea generale, a un altro soggetto interno o esterno alla sua organizzazione. Il Titolare ne monitora lo svolgimento consultandosi con il **Responsabile della Protezione dei Dati** (**RPD**, in inglese *Data Protection Officer* - **DPO**) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del responsabile della sicurezza dei sistemi informativi (*Chief Information Security Officer*, **CISO**) e del responsabile IT.

2.4 Perché la DPIA è così importante?

Lo svolgimento della DPIA offre importanti vantaggi ai fini della **dimostrazione** di **conformità** alla norma, in quanto questa valutazione risulta essere una modalità di analisi efficace per verificare **tutti i principi** di protezione e **gli obblighi** introdotti dal Regolamento.

Tuttavia, lo svolgimento della DPIA non risponde solo ad una esigenza di conformità: una DPIA efficace, infatti, consente di **identificare** e **risolvere** i problemi connessi alla protezione dei dati in una fase precoce, prima dell'avvio del processo di trattamento, portando evidenti benefici in termini di garanzie sia per i soggetti interessati dal trattamento sia all'organizzazione (si pensi agli aspetti connessi con la trasparenza, la reputazione e l'immagine dell'organizzazione stessa).

Lo svolgimento della DPIA costituisce, tra l'altro, una parte **essenziale degli obblighi di un Titolare**: la mancata conduzione della DPIA o un suo svolgimento superficiale può essere sanzionato dall'Autorità competente con ammende amministrative estremamente onerose, fino a € 10 milioni di euro (Art.83 punto 4).

Riferimenti al Regolamento per approfondimenti

Artt. 5 (punto 2), 24, 25, 35, 83

2.5 Come può essere usata una DPIA già svolta?

Una DPIA può concentrarsi su un **singolo** trattamento o **su un gruppo** di trattamenti simili: in caso di DPIA già esistente, **si può fare riferimento** a questa per ogni trattamento di natura similare che presenta rischi analoghi.

In caso di introduzione di **nuove tecnologie**, si può fare riferimento, se la valutazione è ritenuta adeguata, alla DPIA eseguita dallo **sviluppatore del prodotto**.

Per nuovi progetti di trattamento, le DPIA sono una parte vitale della protezione dei dati *by*

design (quindi fin dal progetto iniziale). Un’analisi in questa fase progettuale consente di influenzare lo sviluppo, portando all’attuazione della proposta nel modo più ottimizzato.

Tuttavia, è importante ricordare che le DPIA sono rilevanti anche per i casi di pianificazione di **modifiche a un trattamento esistente**. In questo caso è necessario che il Titolare conduca la DPIA in un momento precedente all’implementazione della modifica.

In altre parole, una DPIA non è semplicemente un timbro di conformità, un tecnicismo da realizzare come parte di un processo di approvazione.

La DPIA è una **valutazione fondamentale** che va integrata nel piano di progetto del nuovo trattamento e mantenuta nel tempo. Quindi, non si deve immaginare una DPIA come un esercizio da svolgere *una tantum* per archiviare poi la pratica. Una DPIA è un processo *vivo e continuativo nel tempo*, introdotto dal Regolamento per aiutare il Titolare a gestire e rivedere periodicamente i **rischi** del trattamento e le misure che sono state messe in atto per mitigarlo.

Riferimenti al Regolamento per approfondimenti

Art.35 (punti 1 e 11) e Considerando n. 84 e 92

2.6 Quale genere di ‘rischio’ deve essere valutato nella DPIA?

Non esiste una definizione esplicita di "rischio" nel Regolamento, ma le varie disposizioni sulla DPIA chiariscono che si tratta di rischi riferiti *agli interessi dei singoli individui*.

L'Art. 35 afferma che un DPIA deve considerare i "*rischi per i diritti e le libertà delle persone fisiche*". Ciò include i rischi per la privacy e i diritti di protezione dei dati, ma anche su altri diritti e interessi fondamentali.

La disposizione chiave della norma su questo tema è espressa nel Considerando 75 presente nel regolamento [GDP1], che collega il **rischio** al concetto di **danno** materiale o immateriale, declinato nella forma di danno **fisico**, danno **economico** e danno **sociale**.

Regolamento – Considerando 75

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un **danno fisico**, materiale o immateriale, in particolare: se il trattamento può *comportare discriminazioni*, *furto o usurpazione d'identità*, *perdite finanziarie*, *pregiudizio alla reputazione*, perdita *di riservatezza dei dati personali protetti da segreto professionale*, *decifratura non autorizzata della pseudonimizzazione*, o qualsiasi altro **danno economico** o **sociale** significativo; se gli interessati rischiano di *essere privati dei loro diritti e delle loro libertà* o venga loro *impedito l'esercizio del controllo sui dati personali* che li riguardano; 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*; in caso di valutazione

di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti *il rendimento professionale*, la *situazione economica*, la *salute*, le *preferenze o gli interessi personali*, *l'affidabilità o il comportamento*, *l'ubicazione o gli spostamenti*, al fine di creare o utilizzare profili personali; se sono trattati dati personali di *persone fisiche vulnerabili*, in particolare minori; se il trattamento riguarda una *notevole quantità di dati personali e un vasto numero di interessati*.

Una DPIA deve valutare, dunque, questo tipo di rischio, e in particolare se esso si manifesta come '*rischio elevato'*. Il Regolamento indica che la **valutazione del rischio** deve essere condotta analizzando la *probabilità* (*likelihood*) di accadimento dell'evento e la *gravità* (*severity*) del danno (o impatto) potenziale che ne consegue.

È importante specificare che, nella Guida che segue, caratterizzeremo con la variabile ***probabilità*** non il semplice 'tentativo' non autorizzato di accedere ai dati da proteggere (senza dunque interessarsi all'esito del tentativo), ma, per fare l'esempio di un attacco malevolo, la *probabilità* dell'evento completo in cui sfruttando una possibile vulnerabilità si riesca ad accedere *effettivamente* ai dati da parte di un soggetto non autorizzato. Questo approccio che indicheremo come 'completo', con riferimento all'esempio ora fatto, è da considerare per tutte le casistiche che si presenteranno nell'analisi, in cui varrà sempre il criterio di valutare, al **contempo,** sia la *minaccia* (cioè il tentativo da parte di qualcuno, dove realizzabile) sia la *vulnerabilità* (cioè la debolezza sfruttata nel sistema di misure messo a difesa dei dati personali).

Riferimenti al Regolamento per approfondimenti

Art.35 (punto 1) e Considerando n. 4, 75, 76, 84 e 90

2.7 Cosa vuol dire 'rischio elevato' e come si può predire questa situazione?

Come detto in precedenza, il *rischio* in questo contesto riguarda i possibili danni materiali o non materiali agli individui, con un rischio declinato nella forma di danno **fisico**, danno **economico** e danno **sociale**.

Per valutare se un trattamento è a "rischio elevato", il Regolamento indica che è necessario considerare sia la *probabilità* sia la *gravità* negli effetti di un determinato evento.

Un "*rischio elevato*" implica, evidentemente, una soglia (quantitativa o qualitativa) più elevata in termini di livello, sia, ad esempio, perché il danno potenziale è più *probabile*, sia perché il danno potenziale è più *grave* (nel senso di più ampio), o anche perché la *combinazione dei due valori* (probabilità e gravità) indica un **livello elevato di rischio** per quel particolare tipo di evento analizzato.

La valutazione **dettagliata** e **affidabile** del livello di rischio, inteso in questo senso, è **uno degli obiettivi fondamentali** della DPIA.

Ma in una **fase preliminare di analisi**, indicata nel seguito come **Fase 0** della valutazione, la

domanda a cui si deve rispondere non è tanto ‘*quanto vale in modo puntuale il rischio per un certo trattamento*’ ma, piuttosto, se *‘il trattamento possa essere caratterizzato da un rischio elevato*’.

Questa sottile, ma sostanziale, differenza è ben indicata nella versione inglese del Regolamento, Art.35 che definisce la DPIA con la frase *“… a processing … is **likely** to result in a high risk*”, con *likely* che assume il significato di probabile/verosimile.

Per svolgere questa analisi preliminare di **Fase 0** ci si potrà servire, se si intenderà seguire le indicazioni di questa Guida, di un ***questionario di screening*** proposto nel prossimo capitolo, in modo da decidere con un approccio sufficientemente analitico ma al contempo rapido, se sia necessaria o meno la DPIA completa per quel trattamento.

Per operare con un *questionario di screening* si cercherà di evidenziare, attraverso le domande poste, se esistono delle “*caratteristiche critiche*” del trattamento, delle *red flags*, come indicano ad esempio le norme del Garante UK, cioè delle *condizioni oggettive,* che la norma e la letteratura tecnica disponibile evidenziano in modo puntuale, alla presenza delle quali **è molto probabile**, seppur *non certo al 100%*, che ci si possa trovare di fronte ad un **trattamento a rischio elevato**.

Importante - Resta comunque valida l’affermazione generale riportata in varie sedi nazionali ed internazionali che, **in caso di dubbio** da parte del Titolare **sul livello di rischio da assegnare** in fase di analisi preliminare, venga deciso di **svolgere comunque la DPIA** nella sua interezza.

[Segue nel prossimo articolo]

Articolo a cura di **Marco Carbonelli**