UNIONE POLIZIA LOCALE ITALIANA
Articolo disponibile all'indirizzo: www.unionepolizialocaleitaliana.it/2021-02/

COME SI ESEGUE LA VALUTAZIONE D'IMPATTO SUL TRATTAMENTO DEI DATI-DPIA

di Massimiliano Mancini (massimiliano.mancini@hotmail.it)[a]

ABSTRACT: *Come svolgere operativamente la DPIA, attraverso un modello schematizzato a fasi per svolgere la Valutazione d'impatto sul trattamento dei dati, obbligatoria in tutti i casi in cui si installa una nuova tecnologia per il trattamento dei dati che può presentare rischi rilevanti per i diritti e le libertà delle persone fisiche, in particolare nei casi obbligatori di adozione di videosorveglianza in sede fissa, su veicoli e su persone, come nel caso delle body cam.*

KEYWORDS: #privacy #GDPR #valutazionedimpatto #valutazioneedimpattosultrattamentodeidatipersonali #dpia #pia #trattamentodatipersonali #DPO #DataProtectionOfficer #RPD #responsabileprotezionedati #massimilianomancini #MassimilianoMancini #EspertiUPLI #UPLI #UnionePoliziaLocaleItaliana

INDICE

PREMESSA

Come è noto il ruolo di titolare del trattamento dei dati è inderogabile, in nessun caso le responsabilità che ne conseguono, incluse quelle per l'omissione degli obblighi di Valutazione d'impatto sul trattamento dei dati, possono essere cedute o mitigate con l'affidamento di incarichi all'interno o all'esterno dell'azienda privata o dell'Ente pubblico da parte del soggetto che ne è legale rappresentante e quindi anche titolare ai fini della privacy.

Il titolare e, in concorso, i responsabili del trattamento e quindi generalmente tutti i funzionari dell'Ente pubblico hanno l'obbligo e la responsabilità della Valutazione d'impatto-DPIA Data Privacy Impact Assessment ogni qual volta si implementa una nuova tecnologia per il trattamento dei dati ed essa, 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 (art.35 c.1 GDPR)[1] e questo può essere rivolto anche all'analisi di un insieme di trattamenti simili che presentano rischi elevati analoghi.

[a] *Segretario Generale UPLI, già comandante dirigente di Polizia Locale e Provinciale, DPO/RPD e consulente privacy in enti pubblici e aziende private esperto in DPIA.*

[1] Reg.UE/2016/679 GDPR, art.35 c.1 (Valutazione d'impatto sulla protezione dei dati) "*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 questo contributo si vuole proporre un metodo per svolgere la Valutazione d'impatto-DPIA procedendo schematicamente per fasi.

QUANDO SI DEVE SVOLGERE LA DPIA IN PARTICOLARE

Come si è già detto in precedenza[2] l'obbligo sussiste specificatamente in tutti i casi di videosorveglianza su aree pubbliche, come previsto dall'articolo 35 comma 1 del Regolamento UE 2016/679 GDPR, e come precisato dal Comitato Europeo per la Protezione dei Dati (*European Data Protection Board – EDPB*) il 29 gennaio 2020, nelle Linee Guida 3/2019 punto 2[3].

L'elenco esteso, anche se non esaustivo, delle tipologie specifiche di trattamenti soggetti al requisito della preliminare Valutazione d'impatto-DPIA è sul sito del Garante per la Privacy all'indirizzo: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058979.

L'omissione dell'obbligo di Valutazione d'impatto-DPIA determina a carico degli enti pubblici così come dei soggetti privati, tra le altre cose, una sanzione sino a dieci milioni di euro (art.35 c.1 e art.83 c.4[4] GDPR), una somma che, anche se applicata in misura ridotta, determina conseguenze devastanti.

CHI DEVE SVOLGERE LA VALUTAZIONE D'IMPATTO SUL TRATTAMENTO DEI DATI

Spetta al titolare del trattamento che nel caso di persone giuridiche si identifica con il legale rappresentante dell'azienda o dell'Ente pubblico, (art.35 c.1 GDPR)[5] che deve consultarsi con il DPO per avere il suo parere (art.35 c.2 GDPR) [6] da indicare nel documento.

Nella decisione sulla realizzazione e nello svolgimento si consulta con il DPO/RDP (Data protection officer/Responsabile per la protezione dei dati) inoltre, se il trattamento lo richiede, può acquisire pareri di esperti, tecnici e in particolare del responsabile della sicurezza dei sistemi informativi (noto anche come Chief Information Security Officer, acronimo CISO) e del responsabile IT (acronimo di Information Technology), laddove presenti, da allegare alla PIA.

Se lo ritiene necessario, il titolare può acquisire anche il parere degli interessati o dei loro rappresentanti purché ciò non pregiudichi gli interessi commerciali o pubblici dell'azienda o ente che

---

[2] Si veda in particolare: https://www.unionepolizialocaleitaliana.it/sito/n20210125/.

[3] EDPB-European Data Protection Board. Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video. Versione 2.0 29 gennaio 2020. Punto 2 Ambito di applicazione "*7. La sorveglianza sistematica e automatizzata di uno spazio specifico con mezzi ottici o audiovisivi per lo più a scopo di protezione della proprietà o per proteggere la vita e la salute delle persone è divenuta un fenomeno significativo dei nostri giorni. Questa attività comporta la raccolta e la conservazione di informazioni grafiche o audiovisive su tutte le persone che entrano nello spazio monitorato identificabili in base al loro aspetto o ad altri elementi specifici. L'identità di tali persone può essere stabilita sulla base delle informazioni così raccolte. Questo tipo di sorveglianza consente inoltre un ulteriore trattamento dei dati personali per quanto riguarda la presenza e il comportamento delle persone nello spazio considerato. Il rischio potenziale di un uso improprio di tali dati aumenta in rapporto alla dimensione dello spazio monitorato e al numero di persone che lo frequentano. Ciò si riflette nel RGPD all'articolo 35 paragrafo 3 lettera c) che impone l'esecuzione di una valutazione d'impatto sulla protezione dei dati in caso di sorveglianza sistematica su vasta scala di un'area accessibile al pubblico e all'articolo 37 paragrafo 1 lettera b) che impone ai responsabili del trattamento di designare un responsabile della protezione dei dati se la tipologia di trattamento per sua natura richiede il monitoraggio regolare e sistematico degli interessati.*".

[4] Reg. UE/2016/679 GDPR, art.83 (Condizioni generali per infliggere sanzioni amministrative pecuniarie) c.4 "*In conformità del paragrafo 2 la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR o per le imprese fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente se superiore: a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8 11 da 25 a 39 42 e 43…omissis…*".

[5] Reg.UE/2016/679 GDPR, art.35 c.1 "*…omissis… 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.".*

[6] Reg.UE/2016/679 GDPR, art.35 c.2 "Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.".

procede e purché non si mettano a rischio i trattamenti stessi che si vogliono valutare con la PIA (art.35 c.9 GDPR)[7].

LO SVOLGIMENTO E L'AGGIORNAMENTO

Il PIA non è un documento statico ma proprio per le sue finalità generali richiede un processo costante di verifica ed eventuale aggiornamento perlomeno quando insorgono variazioni del rischio, secondo il contesto e le evoluzioni tecnologiche, ovvero mutino o si evolvano le attività relative al trattamento.

In questi casi il titolare del trattamento procede a un riesame per valutare se dalle variazioni delle procedure del trattamento che sono intervenute e/o dalle mutate condizioni del contesto ne scaturisca un pregiudizio, anche solo potenziale, sulla sicurezza del trattamento dei dati personali e se le previsioni contenute nel PIA siano ancora valide e attuali (art.35 c.11 GDPR)[8].

LE FASI DI SVOLGIMENTO DELLA VALUTAZIONE D'IMPATTO-DPIA

La normativa in materia e le indicazioni del WP29 (Working Party article 29 o WP29, previsto dall'art. 29 della direttiva europea 95/46)[9] non indicano un modello specifico da adottare, tuttavia le autorità nazionali di controllo hanno fornito degli schemi operativi dai quali si desume il modello che si propone di seguito.

Anche l'International Organization for Standardization (acronimo), l'Organizzazione internazionale per la normazione che è la più importante organizzazione a livello mondiale per la fissazione di norme tecniche, ha pubblicato una linea guida per effettuare un DPIA (ISO/IEC 29134) definendo un processo per la Valutazione d'impatto-Privacy impact assessment con una struttura ed i relativi contenuti del report del DPIA a supporto del principio di accountability.

Per la valutazione del rischio privacy possono essere richiamati gli standard della ISO 31000 che sono citati nel piano nazionale anticorruzione di cui alla Legge 190/2012.

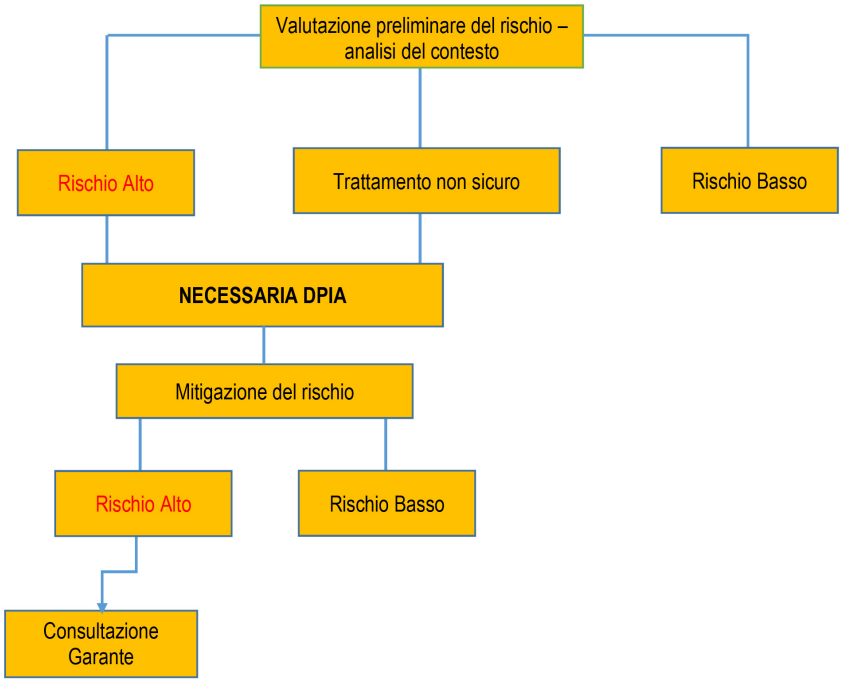
Sulla base di queste premesse si possono definire le seguenti fasi della Valutazione d'impatto-DPIA:

- Fase 1 – Valutazione preliminare della necessità di svolgere la DPIA.
- Fase 2 – Analisi della conformità del trattamento al GDPR.
- Fase 3 – Descrizione del trattamento.
- Fase 4 – Valutazione dei rischi.
- Fase 5 – Analisi del rischio.
- Fase 6 – Il piano di azione.
- Fase 7 – Monitorare il trattamento.

[7] Reg.UE/2016/679 GDPR, art.35 c.9 "Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.".

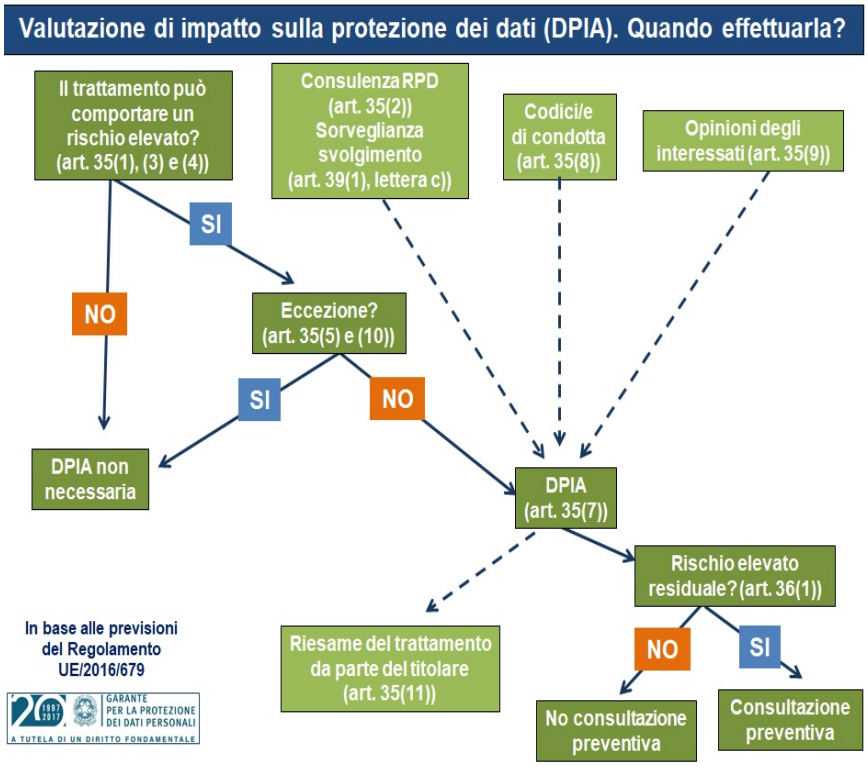
[8] Reg.UE/2016/679 GDPR, art.35 c.11 "Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.".

[9] "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato", realizzate ai fini del regolamento (UE) 2016/679, sono state adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017. Esse sono state stilate dal "Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali", è stato istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995. Le stesse linee guida possono essere consultate al link http://www.interlex.it/2testi/autorit/wp248dpia.pdf.



FASE 1-VALUTAZIONE PRELIMINARE DELLA NECESSITÀ DI SVOLGERE LA DPIA

La fase 1 ha come obiettivo la necessità di stabilire se rispetto ad una determinata attività ricorra o meno la necessità di effettuare una Valutazione di Impatto considerando la natura l'oggetto il contesto e le finalità del trattamento (art.35 c.1 GDPR).



Si tratta di effettuare una analisi del contesto e di condurre una prima analisi che consenta di identificare quali rischi possono manifestarsi nell'esecuzione di un trattamento o quali cause possono renderlo insicuro.

FASE 2-ANALISI DELLA CONFORMITÀ DEL TRATTAMENTO AL GDPR

In questa fase si valuta la liceità delle finalità e del processo di trattamento e quindi il rispetto dei principi di necessità e proporzionalità del trattamento dei dati rispetto alle finalità.

In questo contesto è necessario innanzitutto rendere espliciti gli scopi di impiego dei dati perseguiti con il trattamento e le ragioni delle modalità adottate e gli interessi legittimi del Titolare.

FASE 3-DESCRIZIONE DEL TRATTAMENTO

Al superamento delle due precedenti fasi preliminari, si passa quindi a descrivere il percorso e il ciclo di vita dei dati personali trattati, dalla raccolta all'archiviazione, utilizzo e cancellazione.

La descrizione dei flussi delle informazioni trattate e dei soggetti che possono accedervi è fondamentale per la precisa comprensione dell'intero processo di trattamento dei dati personali al fine di valutare pienamente i rischi ai quali essi sono esposti.

FASE 4-VALUTAZIONE DEI RISCHI

Avendo ben descritto nella fase precedente l'intero ciclo e i singoli passaggi del trattamento dei dati, in questa fase si possono quindi identificare le potenziali minacce alla sicurezza dei dati e alla liceità del trattamento.

L'analisi deve tener conto distintamente delle minacce derivanti da:

- contesto;
- strumenti e sistemi;
- comportamento umano.

FASE 4-ANALISI DEL RISCHIO

È la fase destinata ad identificare le azioni da intraprendere per contrastare i rischi tenendo conto che la DPIA ha come obiettivo la riduzione del rischio o di portarlo ad un livello accettabile.

Funzione del rischio: R=f (C,P)

Il Rischio è da intendersi come la realizzazione di potenziali conseguenze negative e/o non desiderate di un evento e si può esprimere la funzione del Rischio (R) come la combinazione della probabilità (P) e delle conseguenze (impatto) (C) del verificarsi di un particolare evento pericoloso.

La quantificazione dei rischi può quindi essere espressa adottando una funzione del tipo: R=f (C,P) dove R rappresenta il rischio C la gravità delle conseguenze e P la probabilità o la frequenza con cui si verificano le conseguenze.

FASE 6-PIANO DI AZIONE

Il piano di azione rappresenta il supporto e la dimostrazione dell'accountability e consente di definire un piano condiviso delle misure da adottare, delle procedure e delle responsabilità da assegnare nell'esecuzione del trattamento e delle misure di verifica da adottare.

Quindi rappresenta l'assunzione della consapevolezza del Rischio residuo da parte del Titolare del trattamento, dopo aver adottato tutte le misure idonee per ridurre la probabilità e l'impatto e le procedure per mitigare i rischi sul trattamento.

FASE 7-MONITORAGGIO DEL TRATTAMENTO

Le procedure di monitoraggio definiscono la costante verifica e misura dell'accountability.

Questa fase consente, con un costante dialogo e interazione tra Titolare, soggetti Responsabili del trattamento e DPO/RDP di intervenire rapidamente sull'assetto organizzativo in caso di modifiche normative o a seguito dell'evoluzione tecnologica o della necessità di introdurre nuove e più efficaci politiche di gestione dei dati personali.

PER ULTERIORI APPROFONDIMENTI SUL TEMA:

M.Mancini, Illegali gli impianti di videosorveglianza, fototrappole, body cam privi di valutazione d'impatto-DPIA, https://www.unionepolizialocaleitaliana.it/sito/2021-01/

M.Mancini, Nulli e da sanzionare gli accertamenti audiovisivi delle aziende di raccolta rifiuti, https://www.unionepolizialocaleitaliana.it/sito/2021-03/