Fabrizio Di Crosta
Libero professionista
Consulente di direzione e Informatica

Parallelo fra Valutazione rischi privacy e DPIA

Per il **Regolamento UE 679/2016** (*General Data Protection Regulation*, GDPR) la **valutazione dei rischi** sulla protezione dei dati personali (*Processo atto a determinare la probabilità e la gravità del rischio del trattamento, in funzione della natura, dell'oggetto, del contesto e delle finalità del trattamento dei dati personali. La valutazione deve essere basata su elementi di valutazione oggettivi*) è un passaggio fondamentale per garantire che i trattamenti di dati personali avvengano in modo sicuro e conforme alle disposizioni del GDPR stesso.

La valutazione dei rischi privacy – introdotta dal GDPR agli articoli 25 e 32 – comporta l'analisi delle attività di trattamento dei dati personali effettuate dall'organizzazione, al fine di identificare i rischi per i diritti e le libertà degli interessati e stabilire – in base alla ponderazione degli stessi – le misure adeguate per prevenirli. Il GDPR specifica che questa valutazione dei rischi deve avvenire considerando **probabilità** di accadimento di eventi avversi e **gravità** delle conseguenze nel caso si concretizzino i rischi ("*… rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*"). Tale valutazione può essere svolta con varie metodologie, prendendo spunto da standard internazionali (ad esempio norme della serie ISO 31000) o linee guida (Enisa, NIST ecc.), ma l'importante è che siano prese in considerazione minacce, vulnerabilità e sorgenti di rischio che impattano sui dati personali con conseguenze sui **diritti e libertà degli interessati**.

Il Regolamento UE 679/2016 indica che i rischi sono quelli derivanti dai trattamenti dei dati personali, ovviamente quelli mappati e identificati nel Registro delle attività di trattamento ex art. 30 del GDPR. Ogni trattamento può comportare rischi diversi, ma qualora diversi trattamenti di dati personali (ovvero diversi processi dell'organizzazione che trattano dati personali) sono svolti nei medesimi locali e con i medesimi sistemi informatici (gestionali, file server Windows e/o cloud), allora i rischi identificati potrebbero essere considerati come afferenti ai trattamenti di dati personali svolti dall'organizzazione nel suo complesso, considerando il caso peggiore (*worst case*).

Il GDPR richiede anche – all'art. 35 – la **valutazione di impatto** sulla protezione dati (*Data Protec-*

tion Impact Assessment, DPIA), per i trattamenti di dati che presentano un **rischio elevato** per i diritti e le libertà degli interessati (condizione di rischio di pregiudizio dei diritti e delle libertà delle persone fisiche). La DPIA, dunque, è un processo formale e sistematico che consiste nell'analisi delle conseguenze per i diritti e le libertà degli interessati nelle attività di trattamento dei dati personali. Ma non riguarda tutti i trattamenti, solo quelli che a fronte della valutazione complessiva dei rischi hanno portato a un rischio elevato. Il suo obiettivo è quello di garantire che i trattamenti di dati personali più critici per i diritti e le libertà dell'interessato avvengano in modo sicuro e conforme alle disposizioni del GDPR. Oltre ai trattamenti che, a giudizio del Titolare e Responsabile, presentano un rischio elevato, il GDPR ha individuato altre situazioni che configurano la necessità di condurre una valutazione di impatto:

- quando è presente una valutazione sistematica su larga scala basata su trattamenti automatizzati, compresa la profilazione;

- quando vi è un trattamento su larga scala di particolari categorie di dati personali (art. 9) e giudiziari (art. 10);

- quando è presente una sorveglianza su larga scala di zone accessibili al pubblico.

A queste condizioni si aggiungono poi altre situazioni stabilite dalle Autorità di Controllo Nazionali, tra cui anche il GPDP italiano con un Provvedimento dell'ottobre 2018.

La DPIA deve essere effettuata **prima** dell'avvio del trattamento dei dati personali e deve essere documentata. Essa deve contenere una descrizione dettagliata del trattamento dei dati personali, una valutazione dei rischi per la privacy degli interessati e le misure adeguate a prevenirli.
Esistono alcuni modelli e standard per condurre la DPIA: il sistema PIA di CNIL (autorità francese), supportato da un software usufruibile gratuitamente, la ISO 29134, la ISO 29151, il WP 248 (Linee guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati).
La valutazione dei rischi privacy e la valutazione di impatto sono dunque due processi distinti ma complementari nell'ambito della data protection.
Purtroppo si rileva che molte organizzazioni hanno approcciato nel modo errato questo aspetto, scambiando la valutazione di impatto sui trattamenti più a rischio per la valutazione dei rischi generale su tutti i trattamenti. Invece la DPIA è una conseguenza della Valutazione dei Rischi, da condurre solo in determinate situazioni. Riportiamo alcuni esempi di trattamenti che richiedono o non richiedono una valutazione di impatto (ma sicuramente meritano una valutazione del rischio privacy):

- Videosorveglianza. Un impianto aziendale a protezione del perimetro aziendale e degli accessi fisici da malintenzionati non merita una DPIA, una videosorveglianza su una stazione ferroviaria o su un aeroporto necessita di DPIA perché i trattamenti sono su larga scala.

- Una profilazione di utenti che accedono a un sito di e-commerce tipo Amazon necessita di una DPIA.

- La gestione di una Fidelity Card per l'acquisto di beni anche di tipo sensibile (farmaci, parafarmaci, integratori, anche articoli reperibili in un normale supermercato) necessita di una DPIA.

- Il trattamento di dati sanitari di un ospedale effettuato in un processo standard di prenotazione visite ed esami, esecuzione delle visite ed esami diagnostici e refertazione non richiede DPIA in quanto è un trattamento ormai consolidato e normato che richiede solamente l'applicazione di adeguate misure di sicurezza.

In conclusione è importante non confondere i due processi, anche se entrambi comportano una valutazione del rischio, e focalizzare la valutazione sui rischi che corrono i dati personali dell'interessato.