Valutazione del rischio e PIA

Come è noto, il GDPR richiama la valutazione del rischio in due modi:

1. valutazione del rischio per i diritti e le libertà delle persone fisiche per identificare misure tecniche e organizzative adeguate (in questo caso, il GDPR, seppure in modi diversi negli articoli 24, 25 e 32, prevede che questo rischio venga bilanciato con le esigenze del titolare o del responsabile);
2. valutazione degli impatti relativi alla privacy ("Valutazione d'impatto sulla protezione dei dati" o "PIA" o "DPIA" per Data privacy impact assessment).

Pare evidente che si tratta di due cose diverse, altrimenti anche agli articoli 24, 25 e 32 si sarebbe parlato di PIA. Da considerare però che le normative e gli standard non sempre sono scritti in modo da assicurarne la coerenza interna. Sono infatti prodotti da più gruppi di lavoro e frutto di compromessi e alcuni passaggi sono stati introdotti in momenti diversi e senza la cura necessaria per assicurare la coerenza completa con altri punti. Quindi si può immaginare che gli articoli relativi alla PIA siano stati introdotti nel GDPR senza considerarne tutte le relazioni con gli articoli relativi alle misure di sicurezza. Per questo, per esempio, l'articolo 32 (sulle misure di sicurezza) non fa riferimento all'articolo 35 (sulla PIA) e viceversa.

Vale quindi la pena approfondire questi due argomenti per identificarne i punti comuni e le diversità.

Si premette che il testo del GDPR, in molte citazioni, è stato semplificato per assicurare una più facile lettura di questo articolo.

Valutazione del rischio

Agli articoli 24, 25 e 32, il GDPR chiede di stabilire l'adeguatezza delle misure di sicurezza considerando "i rischi per i diritti e le libertà delle persone fisiche" e "lo stato dell'arte e i costi di attuazione, nonché la natura, l'ambito di applicazione, il contesto e le finalità del trattamento". Non chiede espressamente di condurre una valutazione del rischio relativo alla privacy, però è sottinteso che il titolare o il responsabile sappiano dimostrare l'adeguatezza delle misure rispetto a questo "rischio relativo alla privacy".

Il GDPR richiede di bilanciare il rischio del titolare con il rischio degli interessati. Inoltre, il GDPR non richiede di concentrarsi su uno o più trattamenti, ma sulla protezione dei dati personali. È ovvio però che la valutazione deve tenere conto dei trattamenti effettuati (da censire nel Registro delle attività di trattamento).

La valutazione del rischio relativo alla privacy può essere condotta sia a scopo preventivo (per esempio all'inizio di un progetto, con le misure di sicurezza non completamente identificate) sia per identificare il rischio residuo nella situazione attuale.

Si deduce che è possibile valutare il rischio relativo alla sicurezza dei dati personali seguendo i diversi approcci già sperimentati per la sicurezza delle informazioni (anche quando non allineati all'attuale ISO/IEC 27005).

Privacy impact assessment

L'articolo 35 del GDPR richiede venga condotta una PIA per i trattamenti che possono presentare un rischio elevato per gli interessati.

Una PIA deve esaminare un singolo trattamento o trattamenti

simili. Il centro della PIA, quindi, non sono più i dati personali, ma un singolo trattamento.

Il GDPR specifica alcune caratteristiche della PIA. In particolare deve essere documentata riportando:

- la descrizione dei trattamenti;
- la valutazione della necessità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi relativi alla privacy;
- le misure di sicurezza.

Il GDPR suggerisce di raccogliere, per la PIA, le opinioni degli interessati (o dei loro rappresentanti).

La PIA deve essere condotta prima di procedere al trattamento, per identificare eventuali necessità di consultazione dell'autorità garante. Le misure di sicurezza, quindi, potrebbero essere descritte solo in modo generale. Per identificare eventuali rischi residui, nulla vieta (anzi, è consigliato) di condurla anche per trattamenti già attivi per cui è richiesta la PIA dal GDPR.

La PIA, per il GDPR, deve anche valutare se il trattamento potrebbe presentare un rischio elevato supponendo l'assenza di misure di sicurezza (utilizzando approcci classici di valutazione del rischio, è necessario considerare solo il valore dei dati e la verosimiglianza di una minaccia, senza considerare le misure che ne riducono l'impatto o ne prevengono il successo).

Strumenti

Tralasciando gli strumenti software prodotti da molte società di consulenza (solitamente poco efficienti), è opportuno considerare alcuni testi che trattano di PIA e valutazione del rischio privacy.

Il primo è lo standard internazionale ISO/IEC 29134 dal titolo

“Guidelines for privacy impact assessment”. Esso specifica che la PIA riguarda programmi, sistemi informatici o processi e solo in alcuni punti ricorda di analizzare i processi. Al centro di questo standard non ci sono i trattamenti (anche se sarebbe facile e non scorretto leggerlo in questa ottica), ma gli asset.

La ISO/IEC 29134 ricorda molto la guida del CNIL (il Garante francese), che è invece più orientata ai trattamenti.

Il CNIL ha anche pubblicato un software per la conduzione di una PIA. Esso è in realtà un modello di documento che indica quali argomenti trattare in ciascun capitolo del rapporto di PIA.

Altro documento interessante è il “Handbook on Security of Personal Data Processing” di ENISA. Il documento non nomina quasi mai la PIA, ma presenta un metodo molto semplice e pragmatico per la valutazione del rischio dei trattamenti. Gli esempi di applicazione sono proprio sui trattamenti.

Il WP Art. 29, fonte autorevolissima, con il documento WP 248 (aggiornato il 4 ottobre 2017) non propone alcun metodo, ma fornisce i “criteri per una DPIA accettabile”. Tra le altre cose, il WP 248 dichiara l’importanza di valutare il rischio anche quando si decide di non effettuare una PIA, lasciando intendere, quindi, che si tratta di due cose diverse.

Sono stati pubblicati numerosi altri documenti. Alcuni, usando scorrettamente il termine PIA, presentano delle check list di base sugli adempimenti del GDPR o dei commenti sul GDPR o dei metodi di pianificazione e attuazione degli adempimenti privacy.

Negli anni precedenti alla pubblicazione del GDPR e alla proliferazione di documenti relativi alla PIA, erano facilmente reperibili dei documenti denominati “Privacy impact assessment” molto simili alle informative privacy, ossia con una descrizione dei trattamenti, dei rischi e delle misure di

sicurezza in formato libero, senza calcoli di sorta. Questo approccio “libero” non è da escludersi a priori, anche se al momento non promosso.

Allora, quali sono le differenze?

Per come sono descritte, è sicuramente possibile costruire una valutazione del rischio privacy come l’insieme delle PIA relative ai trattamenti effettuati. Viceversa, si può elaborare una PIA come sottoinsieme della valutazione del rischio privacy, ricordandosi però di valutare gli impatti solo per gli interessati e, dove possibile, coinvolgere gli interessati. Gli algoritmi di calcolo possono essere i medesimi (questa opzione, ovviamente, non è perseguibile se la PIA è presentata in formato “libero”).

Alla luce di tutto ciò si può quindi concludere che la valutazione del rischio privacy e la PIA non presentano differenze tecniche sostanziali, ma è sempre e comunque necessario ricordare i loro diversi obiettivi (in particolare il fatto che la PIA deve indicare quando è necessaria la consultazione preventiva con il Garante) e le piccole, ma significative, differenze.

A cura di: **Cesare Gallotti**

L’articolo Valutazione del rischio e PIA proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/valutazione-del-rischio-e-pia/