DPIA tra GDPR e prassi

La prospettiva di un DPO

Fabrizio Venturelli

Sr. Director - Global DPO

Workday

Agenda

01 Introduzione alla DPIA

02 DPIA & DPO

03 Quando serve

04 Che cosa deve contenere

05 DPIA & Matrice di rischio

06 Opinione degli interessati

07 Consultazione preventiva

08 DPIA: il processo circolare

09 Case studies

DPIA - Introduzione

- Che cos'è una DPIA - Data Protection Impact Assessment / Valutazione dell'impatto sulla protezione dei dati
  - Art. 35
    - Comma 1.
      - *"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* (...)".

DPIA & DPO

- Il ruolo del DPO in riferimento alla DPIA
  - Art. 35 / 39
    - Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si **consulta con il responsabile della protezione dei dati (DPO)**, qualora ne sia designato uno. Il DPO deve godere della massima **indipendenza.**
    - Il DPO deve avere la possibilità di riferire al vertice organizzativo del titolare (es. CdA, Avvocato Generale)
    - Linee Guida EDPB: Qualora il titolare decida di non seguire l'opinione del DPO deve essere documentata formalmente la ragione.
    - Il DPO può riferire all'autorità se ritiene che il rischio per i soggetti interessati sia troppo alto

DPIA - Quando serve

- Necessità di effettuare una DPIA
  - Art. 35
    - Comma 3:
      - Una DPIA si rende necessaria nei seguenti casi:
        - trattamenti sistematici, globali, automatizzati, compresa la profilazione sulla quale si fondano decisioni che abbiano effetti giuridici o che incidono significativamente su persone giuridiche
        - il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o articolo 10 (es. Art. 9 Dati relativi alla salute, orientamento sessuale, politico, razza o religione e art. 10 dati personali relativi a condanne penali e a reati)
        - la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (e.s. CCTV)

DPIA - Che cosa deve contenere (I)

- Contenuti della valutazione del rischio
  - Art. 35
    - Comma 7:
      - La DPIA deve contemplare almeno
        - La descrizione dettagliata dei trattamenti (finalità e interesse legittimo ove applicabile)
        - Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità
        - Valutazione dei rischi per i diritti e libertà degli interessati
        - Misure di mitigazione del rischio (es. misure di sicurezza)

DPIA - Che cosa deve contenere (II)

- Contenuti della valutazione del rischio
  - Considerando 84, 90 - principi rilevanti
    - Mitigazione
    - misure appropriate
    - stato dell’arte delle tecnologie disponibili
    - costo eccessivo della mitigazione, impossibilità di mitigazione
    - valutazione del rischio (gravità dell’impatto / probabilità dell’avverarsi del rischio)

DPIA - Matrice di rischio

More ← HAZARD PROBABILITY → Less

More ↑ HAZARD SEVERITY ↓ Less

	A Frequent	B Probable	C Occasional	D Remote	E Improbable
1 Catastrophic	High	High	High	High	Medium
2 Critical	High	High	High	Medium	Low
3 Marginal	High	Medium	Medium	Low	Low
4 Negligible	Medium	Low	Low	Low	Low

Reduce Severity and Likelihood

DPIA - Opinioni degli interessati

- Il titolare raccoglie le opinioni degli interessati “se del caso”
  - Art. 35
    - Comma 9:
      - Spesso necessario se gli interessati siano potenzialmente in numero molto elevato, se il trattamento possa porre ad alto rischio i loro diritti o libertà, ma anche se il titolare ritenga che possa essere vantaggioso anticipare questo "contraddittorio" prima di iniziare il trattamento e anche per, eventualmente, rendere più “difendibile” la propria posizione con l’autorità di controllo se la consultazione preventiva fosse necessaria.

Modalità di consultazione:
- Studi di ricerca
- Coinvolgimento delle associazioni di categoria
- Sondaggi rivolti ai potenziali utenti / soggetti interessati

Se il titolare decidesse:
a. Di procedere in modo difforme dalle opinioni degli interessati o
b. Di non procedere alla consultazione

dovra’ documentare e motivare/ giustificare tale decisione.

La consultazione preventiva della DPA competente

L’Autorità di controllo quando scopre che non avete mitigato i rischi per i soggetti interessati e chiedete se potete comunque iniziare il trattamento

L’azienda pronta a lanciare il prodotto alla prima riunione con la DPA

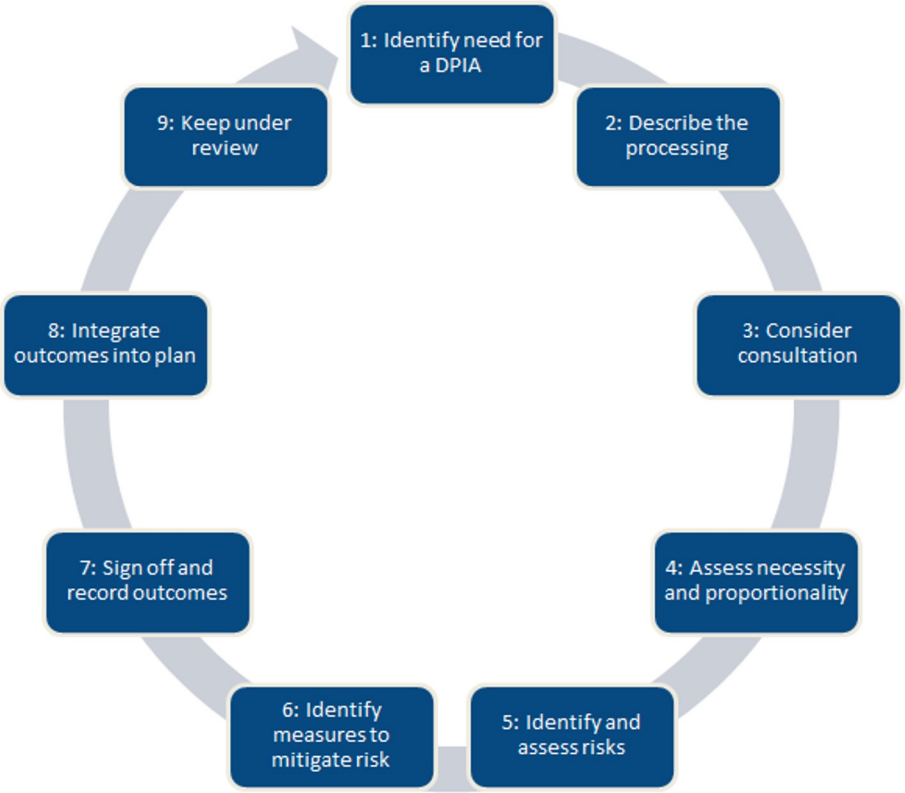
DPIA - Consultazione preventiva

- Quando è necessario coinvolgere l'Autorità di controllo
  - Art. 36
    - Il titolare, prima di procedere al trattamento consulta la DPA
      - Rischio elevato per i soggetti interessati
      - In assenza di misure di mitigazione
    - Segue un procedimento di consultazione con specifici termini di cui al comma 2, in cui la DPA fornisce indicazioni ed eventualmente può approvare, a certe condizioni, o negare il trattamento a seconda degli esiti della consultazione

DPIA - Pubblicazione

- Non necessaria, ma consigliata dalle linee guida EDPB
  - Molte grandi compagnie seguono questa *best practice*
    - Per costruire un rapporto fiduciario con il pubblico / soggetti interessati
    - Particolarmente indicata nel caso di enti pubblici
    - Può essere un estratto dell'intera DPIA
      - Bilanciamento con obblighi / opportunità di confidenzialità e segretezza a livello aziendale

DPIA - Il processo



- E' un processo suddiviso in fasi da tenere monitorato con continuità
- Non è una valutazione da eseguire *una tantum*

*Immagine tratta dal sito del UK ICO (Autorità di controllo inglese)

Case studies

1. App di incontri
   a. Azienda X negli USA sviluppa un'app di incontri
   b. L'Azienda ha lanciato il prodotto nel mercato americano e ha molti clienti negli USA
   c. La app raccoglie con consenso, tutti i dati che l'utente fornisca.
   d. Inoltre la privacy policy della app, per la quale non e' richiesta alcuna visione da parte dell'utente, specifica brevemente che il GPS, i dati della rubrica, i dati di navigazione di app terze (es. browsers) sono raccolte per migliorare il servizio.
   e. La app utilizza Google Analytics, ovvero si avvale di cookies per migliorare la performance del prodotto e questo viene menzionato nella privacy policy specificando che Analytics non si puo' disattivare.
   f. La app inoltre funziona tramite un algoritmo che in modo estremamente efficiente ed automatizzato elabora e migliora nel corso del tempo il profilo degli utenti, incrociando i loro dati personali anche con siti di social network in modo da offrire il miglior matching possibile con eventuali partner.
   g. I dati sono conservati per un periodo di tempo indeterminato. Se l'utente lo desidera però può disinstallare l'app in ogni momento.
   h. Per accedere ai dati che non siano esclusivamente quelli del profilo bisogna fare una richiesta di accesso che può richiedere fino ad un mese per essere eseguita da un team dedicato.

   ⇒ Che cosa dovete considerare nella DPIA?
2. App per la gestione della performance lavorativa
   a. Un'Azienda americana ha sviluppato un software estremamente efficiente nella valutazione della performance lavorativa che per il suo funzionamento accede ad una serie di funzionalita' del computer aziendale del dipendente nonché al badge ed alle telecamere aziendali, in modo da poter monitorare con estrema precisione il comportamento ed il rendimento del personale.
   b. L'Azienda in questione ha un cliente in Italia.
   c. Il DPO dell'azienda cliente italiana è contemporaneamente anche l'impiegato addetto alla sicurezza e allo sviluppo del software in questione
   d. Il software in questione al momento del lancio permette di chiedere il consenso informato al lavoratore per potere essere "monitorato"; inoltre una policy sul funzionamento dettagliato del monitoraggio è disponibile sul sito web dell'azienda di sviluppo software.
   e. Il monitoraggio permette al datore di lavoro di individuare dipendenti considerati pigri o meno meritevoli di promozioni.

   ⇒ Che cosa dovete considerare nella DPIA?

Thank You