

DATA PROTECTION IMPACT ASSESSMENT

Tra obbligo e opportunità

DI COSA SI TRATTA?

DPIA O valutazione d'impatto o data protection impact assessment o semplicemente assessment:
è una **procedura di autovalutazione** che il regolamento n.679/2016 in materia di trattamento dati personali impone di effettuare al titolare del trattamento e in alcuni casi anche al responsabile del trattamento, quando ricorrono determinate circostanze nel trattamento dei dati personali trattati

DPIA UN'OPPORTUNITA' ORGANIZZATIVA

La DPIA in ogni caso non deve essere vista esclusivamente come un'imposizione cui adeguarsi per evitare sanzioni e quindi un obbligo giuridico, ma come un'opportunità organizzativa

PERCHE' UNA DPIA

Grazie a questa procedura un'azienda potrà ripensare la propria struttura organizzativa, rendendola eticamente superiore e più trasparente, migliorando la propria immagine e la propria reputazione agli occhi del suo pubblico e degli stakeholders - di clienti, fornitori, partner commerciali, dipendenti, p.a., banche - in quanto una DPIA è **un modo eccellente per dimostrare che un'azienda tratta correttamente e in maniera sicura e accurata i dati personali.**

VANTAGGI DPIA ESTERNI

1. MIGLIORAMENTO IMMAGINE AZIENDALE

le persone risulteranno rassicurate sul fatto che l'organizzazione che ha condotto una DPIA, usa di certo le informazioni secondo delle best practice. Un **progetto, un processo, un'app o un prodotto che sono stati oggetto di una DPIA sono sicuramente meno invasivi rispetto alla privacy** e quindi vi saranno meno probabilità di influenzare negativamente i diritti e le libertà delle persone.

VANTAGGI DPIA ESTERNI

2. MAGGIORE TRASPARENZA

una DPIA consente **maggiore trasparenza sul modo in cui i dati personali vengono trattati**, rendendo agli interessati più facile comprendere come e perché le loro informazioni vengono utilizzate da un'organizzazione.

VANTAGGI DPIA INTERNI

3. MIGLIORAMENTO ORGANIZZATIVO

Anche l'impresa trarrà beneficio dal condurre una DPIA non solo da un punto di vista della brand reputation, ma anche da un punto di vista interno, in quanto avrà un'organizzazione più preparata ad affrontare eventuali situazioni incresciose, come ad esempio una violazione sui dati personali, in quanto, **grazie ad una valida ed efficace DPIA, avrà già preordinato come comportarsi in tali circostanze e potrà intervenire speditamente**

VANTAGGI DPIA INTERNI

Condurre una DPIA, infatti consente:

- a. di identificare un problema in anticipo e questo comporta generalmente una soluzione più semplice e meno costosa;**
- b. ridurre i costi di un progetto in corso, minimizzando la quantità di informazioni che vengono raccolte o utilizzate laddove possibile ed elaborando processi più diretti per i dipendenti.**

VANTAGGI DPIA INTERNI

Più in generale, l'uso coerente delle **DPIA** **aumenta la consapevolezza** delle questioni relative alla **privacy** e alla protezione dei dati all'interno di un'organizzazione e garantisce che tutto il personale coinvolto nella realizzazione dei progetti rifletta sulla privacy già dalle prime fasi di ideazione, rispettando anche il principio della **privacy by design e default**

VANTAGGI DPIA ANCHE PER CHI NON E' OBBLIGATO

Da ciò si comprende che una DPIA potrebbe essere un valido supporto anche se non si rientra nei casi per i quali condurla è un obbligo di legge, essa infatti potrebbe essere applicata a qualsiasi progetto che includa un trattamento di dati personali.

CASI DI ESEMPIO IN CUI E' OPPORTUNO CONDURRE UNA DPIA

Si pensi all'implementazione di un nuovo sistema di videosorveglianza (specialmente quello che monitora i membri del pubblico) o all'applicazione di una nuova tecnologia a un sistema esistente (ad esempio aggiungendo funzionalità di riconoscimento automatico della targa delle autovetture che entrano in un determinato luogo alle telecamere a circuito chiuso esistenti), oppure si pensi ad un nuovo database che riorganizza i dati personali secondo il comportamento d'acquisto degli utenti.

DPIA. QUANDO E' OBBLIGATORIA

E' l'art. 35 punto 3 del regolamento che fissa le circostanze in cui è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati trattati, stabilendo al comma 1 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.

DPIA. QUANDO E' OBBLIGATORIA

TRATTAMENTI CHE POSSONO PRESENTARE RISCHI ELEVATI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI.

UNA SINGOLA DPIA PUO' ESSERE SUFFICIENTE PER TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI

DPIA. QUANDO E' OBBLIGATORIA

Più in dettaglio, la valutazione d'impatto sulla protezione dei dati personali è richiesta in particolare nei casi seguenti:

- trattamenti automatizzati, compresa la profilazione e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente sulle persone fisiche (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento);
- trattamenti, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 (trattamento di dati cosiddetti sensibili), o di dati relativi a condanne penali e a reati di cui all'articolo 10 (trattamento di dati giudiziari);
- Videosorveglianza sistematica su larga scala di una zona accessibile al pubblico

TIPOLOGIE TRATTAMENTI DA SOTTOPORRE A DPIA

Il Garante, anche nel rispetto di quanto stabilito dal GDPR sta lavorando per la redazione e la pubblicazione di un elenco di tipologie di trattamenti soggetti al requisito della DPIA, in quanto trattamenti basati sulle nuove tecnologie (es. trattamenti che utilizzano nuovi strumenti legati all'industria 4.0 o trattamenti svolti attraverso l'IoT), anche se la legge di bilancio 2018 ha imposto per tali tipologie di trattamento di mantenere la notifica preventiva al Garante quando il trattamento si basa sull'interesse legittimo del titolare.