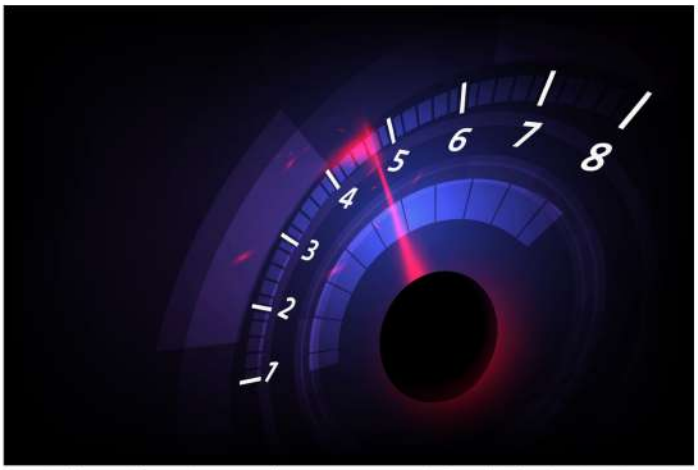
La valutazione di impatto sulla protezione dei dati (DPIA): il fai da te è possibile?

LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (IN INGLESE "DPIA", DA "DATA PROTECTION IMPACT ASSESSMENT") È UN ADEMPIMENTO OBBLIGATORIO MA ANCHE UN IMPORTANTE STRUMENTO DI ACCONTABILITY, IN QUANTO CONSENTE ALLE ORGANIZZAZIONI DI DIMOSTRARE CHE UN DETERMINATO TRATTAMENTO È STATO VALUTATO E RISULTA CONFORME AGLI OBBLIGHI PREVISTI DAL REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (GDPR).

Federico Corti
Luglio 27, 2022
Scarica PDF dell'articolo



Quando effettuare la/il DPIA (**Data Protection Impact Assessment**)? È possibile fare da soli? Se si, come? Dalle ultime sanzioni ricaviamo alcune considerazioni utili.

PREMESSA: COSA SI INTENDE PER DPIA E QUANDO È OBBLIGATORIA

Ai sensi dell'art. 35 del GDPR, la DPIA rappresenta un processo volto ad analizzare un determinato trattamento in modo da stimare, in una prima fase, in relazione alla probabilità e alla gravità, i rischi per i diritti e le libertà delle persone fisiche e, in una seconda fase, a trattare i **rischi**, definendo le misure per escluderli o per attenuarli.

L'obbligo della DPIA, per sua natura, non può quindi considerarsi un mero **adempimento burocratico**: si tratta, piuttosto, di uno strumento di gestione del rischio in grado di produrre un indubbio vantaggio per il titolare che, affrontando i profili di protezione dei dati prima che abbia inizio il trattamento alla base di un prodotto, un'applicazione o di un servizio, riduce l'incertezza giuridica relativa ai rischi, anche a beneficio degli interessati/utenti.

Il GDPR non richiede sempre la valutazione di impatto, ma solo se un determinato trattamento, tenuto conto della natura, della portata, del contesto e della specifica finalità, è suscettibile di causare un rischio elevato per i diritti e le libertà delle persone fisiche. L'**"indeterminatezza nella definizione di "rischio elevato"** ha spinto il Gruppo di lavoro ex art. 29 (oggi European Data Protection Board) ad individuare nove criteri, che costituiscono degli indici rilevanti per il titolare che deve assumere la propria determinazione sul punto. Sulla base dei nove criteri ed *"allo scopo di specificarne ulteriormente il contenuto"* il Garante ha sviluppato un proprio elenco, composto da dodici tipologie di trattamenti soggetti al requisito di una valutazione d'impatto.

Il Gruppo di lavoro ha precisato che, in caso di dubbio in ordine alla necessità di procedere o meno con la DPIA, **è sempre opportuno realizzarla**. Nel caso in cui il titolare decidesse di non realizzarla, è bene che sia in grado di giustificare e documentare le ragioni che lo hanno spinto a prendere questa decisione.

CONTENUTO E VALUTAZIONE DEI RISCHI

L'art. 35, al paragrafo 7, prevede che la valutazione contenga, almeno:

- *"a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento".*

In primo luogo, quindi, **trattamento e finalità** devono essere descritti in modo completo, coerente, chiaro e non generico.

- *"b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità".*

Rispetto alle finalità individuate e perseguite, la DPIA richiede una valutazione circa la necessità e la proporzionalità del trattamento. In questa fase dovrebbe essere valutata l'efficacia del trattamento stesso, che deve poter essere ragionevolmente idoneo a perseguire la finalità.

- *"c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1".*

Questo è, probabilmente, il punto più complesso: identificare e gestire i rischi implica un processo di analisi, stima, valutazione, mitigazione e riesame degli stessi. Processo che dev'essere svolto considerando l'insieme di circostanze particolari del trattamento e l'insieme di dati raccolti e trattati. Inoltre, sono diverse e molteplici le fonti in materia di valutazione dei rischi, così come sono diverse le metodologie (si citano, in particolare, la ISO guide 71:2009; la ISO ISO/IEC 29134:2017 contenente linee guida per il Privacy Impact Assessment e le altre norme internazionali sul risk management ISO 31000:2010 e 27005:2011).

- *"d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione".*

Qualunque sia la metodologia prescelta, la valutazione dei rischi dovrebbe consentire l'individuazione di

garanzie, misure di sicurezza e meccanismi per assicurare la protezione dei dati ed il rispetto del GDPR.

LA SANZIONI

In caso di inosservanza delle disposizioni dell'articolo 35 (sulla valutazione d'impatto) e dell'articolo 36 (sull'istituto della consultazione preventiva, da attuare nel caso in cui dalla DPIA si evinca un rischio elevato in assenza di misure idonee ad attenuarlo), il titolare rischia 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. In diverse occasioni l'Autorità Garante ha già sanzionato per la violazione delle norme relative alla DPIA.

L'ultima ordinanza di ingiunzione comminata dal Garante, con particolare riferimento alla violazione dell'art. 35, riguarda l'Azienda ospedaliera di Perugia (provv. n. 134 del 7 aprile 2022). L'Azienda ospedaliera, mediante l'applicativo per il whistleblowing ha operato un trattamento in assenza di una preliminare valutazione d'impatto sulla protezione dei dati. L'Autorità ha specificato che "*tenuto conto delle indicazioni fornite anche a livello europeo, il trattamento dei dati personali mediante i sistemi di acquisizione gestione delle segnalazioni presenta rischi specifici per i diritti e le libertà degli interessati, considerata anche la particolare delicatezza delle informazioni potenzialmente trattate, la "vulnerabilità" degli interessati nel contesto lavorativo, nonché lo specifico regime di riservatezza dell'identità del segnalante previsto dalla normativa di settore*". La carenza della valutazione d'impatto non ha consentito all'organizzazione di individuare misure specifiche per attenuare i rischi derivanti dal trattamento, pertanto il Garante ha comminato una sanzione di importo complessivo pari a 40.000 euro.

- In questo caso, è importante evidenziare il fatto che la non conformità si sia verificata a monte: il titolare del trattamento non ha saputo individuare l'esigenza stessa della DPIA. Una valutazione dei rischi, infatti, avrebbe consentito all'organizzazione di soppesare gli elevati rischi, in termini di possibili effetti ritorsivi e discriminatori, anche indiretti, per il segnalante (la cui identità è protetta da uno specifico regime di garanzia e riservatezza, previsto dalla normativa in materia di whistleblowing) e di determinare chiaramente l'esigenza della valutazione d'impatto.

Il 13 gennaio 2022 il Garante ha sanzionato l'Azienda sanitaria unica regionale Marche per un importo pari a complessivi 14.000 euro, per violazione dei principi di integrità e riservatezza, degli obblighi del titolare del trattamento in materia di sicurezza del trattamento e di valutazione d'impatto sulla protezione dei dati (provv. n. 9 del 13 gennaio 2022). L'istruttoria è partita da una notizia stampa che evidenziava una vulnerabilità nel sistema di acquisizione e gestione dei dati dello screening del Covid-19: a causa dell'errata configurazione dell'APP "Smart4You" chiunque poteva facilmente accedere al profilo sanitario di un'altra persona.

- In questo caso, il titolare, seppur consapevole degli obblighi previsti dal GDPR, ha considerato l'attività svolta come una semplice integrazione tra prenotazione e refertazione (servizi preesistenti). Se il titolare avesse riconosciuto il trattamento come distinto rispetto alle altre finalità perseguite, avrebbe potuto condurre una valutazione dei rischi sullo stesso, riconoscendo l'effettiva necessità di DPIA.

Un altro provvedimento interessante è sicuramente l'ordinanza di ingiunzione dei confronti dell'Università Commerciale "Luigi Bocconi" di Milano (n. 317 del 16 settembre 2021). Diverse violazioni sono state rilevate in relazione all'impiego di un sistema di supervisione (proctoring) nell'ambito dello svolgimento delle prove scritte d'esame degli studenti, al fine di identificare questi ultimi e/o di verificarne il corretto comportamento durante lo svolgimento della prova d'esame.

- In questo caso, il titolare ha condotto una DPIA sul sistema. Tuttavia il Garante, dall'esame della documentazione, ha rilevato che, la valutazione di impatto, "*non è stata condotta in maniera del tutto adeguata, limitandosi a illustrare le caratteristiche del sistema di supervisione utilizzato, rappresentandolo come conforme al quadro normativo in materia di protezione dei dati, senza però una puntuale valutazione "della necessità e proporzionalità dei trattamenti in relazione alla finalità" e "dei rischi per i diritti e le libertà degli interessati" (art. 35, par. 7, lett. b) e c)]*". In particolare, l'Autorità ha rilevato i seguenti aspetti come non conformi:
- I giudizi di adeguatezza estremamente sintetici, privi di idonea motivazione;
- La mancata individuazione, in relazione a taluni profili, di appropriate misure "per affrontare i rischi" e per attenuare gli stessi, oppure la presenza di misure "inconferenti per la mitigazione del rischio";
- La mancata puntuale valutazione in merito all'adeguatezza, alla pertinenza e alla proporzionalità di ciascuna categoria di dati oggetto di trattamento;
- La mancata effettiva valutazione circa le possibili ripercussioni per gli interessati in caso di errori o falsi positivi/negativi generati dallo strumento di supervisione;
- In generale, la presenza nella DPIA di dichiarazioni superficiali (ad es. "non si potrebbe determinare discriminazione alcuna") non sostenute da argomentazioni a sostegno (quale una previa valutazione sull'affidabilità degli algoritmi utilizzati dal sistema di supervisione).

10 STEP FONDAMENTALI

Le sanzioni esaminate mostrano come le non conformità possano annidarsi in diverse fasi:

- Nella fase preliminare di mappatura dei trattamenti svolti;
- Nella fase di valutazione dei rischi, per determinare se la DPIA è necessaria o meno;
- Nella fase di sviluppo della DPIA.

Per questo è opportuno ricordare in sintesi quelli che sono i principali step da seguire per adeguare i trattamenti al GDPR e agli obblighi derivanti dall'art. 35:

1. mappare tutti i trattamenti, individuando le specifiche finalità che si intende perseguire;
2. effettuare una preventiva valutazione dei rischi per ciascun trattamento;
3. determinare, in base al dettato della norma, alle linee guida delle Autorità, nonché ai rischi rilevati, se è obbligatoria o comunque opportuna la valutazione d'impatto;
4. verificare se il trattamento ricade fra le eccezioni di cui all'art. 35 par. 5 e par. 10;
5. coinvolgere il RPD | DPO, ove presente;
6. Se del caso, raccogliere 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;
7. condurre la DPIA, anche con l'ausilio di eventuali tools o template, oppure giustificare la scelta di non procedere in tal senso;
8. considerare nella valutazione gli eventuali codici di condotta approvati;
9. Se all'esito della DPIA vi è un rischio residuo elevato, valutare la possibilità di andare in consultazione preventiva (art. 36 GDPR), riprogettare oppure interrompere il trattamento;
10. Se necessario, 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.

FRA TOOLS E TEMPLATE, IL FAI DA TE È POSSIBILE?

Nel condurre la valutazione d'impatto, i titolari del trattamento hanno a diposizione diversi strumenti che, nel tempo, sono stati rilasciati dalle Autorità di controllo. Fra tutti, lo strumento più conosciuto e, probabilmente, anche quello più utilizzato, è il tool della CNIL francese (la "Commission nationale de l'informatique et des libertés"), che si configura come un vero e proprio applicativo open source, di facile installazione ed utilizzo. Il Garante per la protezione dei dati personali ha collaborato alla implementazione della versione in lingua italiana dello strumento e ha messo a disposizione una breve guida all'installazione, nell'area tematica del sito istituzionale.

Altre Autorità, hanno preferito fornire dei template: fra tutti si rinvia alla guida del BfDI (Garante tedesco); alle indicazioni dell'ICO (Garante inglese), che ha pubblicato un "self-assessment toolkit"; al documento informativo dell'AEPD (Garante spagnolo).

Sono quindi diverse le metodologie che può seguire il titolare per condurre la valutazione d'impatto. Come si evince dalle sanzioni sopra analizzate, tuttavia, seguire le metodologie standardizzate dalle Authority è importante ma non basta. Anche il Garante ha dichiarato, in merito al software della CNIL, che "*Il software qui presentato NON costituisce un modello al quale fare riferimento in ogni situazione di trattamento [...]». Potrebbe costituire quindi un utile supporto di orientamento allo svolgimento di una DPIA, ma non va*

inteso come schema predefinito per ogni valutazione d'impatto che va integrata in ragione delle tipologie di trattamento esaminate".

Il riscontro ai punti richiesti dall'art. 35 par. 7, nonché alle domande di dettaglio dei tools utilizzati, deve essere quanto più accurato possibile, ogni aspetto che sia suscettibile di impattare sul trattamento svolto e sui dati degli interessati deve essere considerato. Nella valutazione è bene prendere in considerazione tutte le fonti applicabili in materia e le linee guida delle principali Authority.

L'esperienza, in questo campo, è ciò che fa la differenza fra l'essere in regola e l'averci provato.

Il prossimo anno Labor Project potrà vantare ben vent'anni di esperienza sul campo. Contattaci per farti seguire nella realizzazione della valutazione di impatto, o per capire, insieme ai nostri consulenti, quali trattamenti presentano un rischio alto e devono essere adeguati.

Per qualsiasi dubbio il nostro team è a tua disposizione!

Labor Project®
consulenza operativa per l'impresa

Labor Project S.r.l.
Iscrizione Ufficio Registro Imprese
di Como con n. 02725120139
Cap. Soc. € 100.000 i.v.
P.I. 02725120139

CANTU'
Via Brianza, 65
22063 Cantù (CO)
Tel. +39 031 704381
info@laborproject.it

ROMA
Via Lima, 7
00198 Roma (RM)

roma@laborproject.it

MILANO
Viale Monza, 347
20126 Milano (MI)

milano@laborproject.it

LUGANO
Via Luigi Canonica,11
6900 Lugano (Svizzera)

info@privacydesk.ch