DPIA e GDPR: che c'è da sapere per una corretta valutazione dei rischi privacy

LA GUIDA COMPLETA

Diego Padovan
Data Protection Officer, Amministratore DPO Compliance Consulting.

Realizzare correttamente una DPIA consente al titolare del trattamento di gestire al meglio il rischio che incombe sui dati personali. Ecco come procedere ad una pertinente ed efficiente valutazione dei rischi privacy

La sezione 3 del GDPR e l'art. 27 della direttiva (Ue) 2016/680 introducono la valutazione d'impatto sulla protezione dei dati personali (DPIA secondo l'acronimo inglese Data Protection Impact Assessment), con riguardo a un trattamento che può presentare un rischio privacy elevato per i diritti e le libertà delle persone fisiche.

Eppure, in generale, **un trattamento di dati personali non è classificabile a priori come a rischio elevato**, a meno che non rientri nelle ampie categorie descritte dal GDPR, in particolare dei trattamenti:

- su larga scala;
- di profilazione;
- di sorveglianza di zone accessibili al pubblico su larga scala (in particolare se effettuata mediante dispositivi optoelettronici);
- che prevedono l'utilizzo di un grado di conoscenza tecnologica elevato;
- che prevedono l'utilizzo di categorie particolari di dati;
- che prevedono l'utilizzo di dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza;

oppure, ancor più in generale, di trattamenti che rendono più difficoltoso l'esercizio dei diritti degli interessati o di avvalersi di un servizio o di un contratto.

Pertanto, per comprendere se i trattamenti effettuati dal titolare del trattamento rientrino o meno nella casistica degli esempi appena elencati, o siano valutabili comunque come ad alto rischio, è necessario un processo ad hoc, che tenga sempre in considerazione il rischio come relativo ai diritti e le libertà dell'interessato, non del titolare del trattamento.

DPIA e GDPR: chi deve eseguire la valutazione e come

A tal fine, è utile analizzare l'Art. 35 del GDPR e individuarne le parole chiave: *"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"*.

Dall'art.35 emerge chiaramente **che il soggetto cui spetta il compito di gestire il rischio che incombe sui dati personali e valutarne il livello è il titolare del trattamento**, coadiuvato dal supporto specialistico da parte del Responsabile della Protezione dei Dati (RPD o DPO in inglese). Inoltre, come suggerito dallo stesso Garante, la conduzione materiale della valutazione di impatto può essere affidata ad un altro soggetto,

interno o esterno all'organizzazione, acquisendo, se i trattamenti lo richiedono, il parere di esperti di settore, del responsabile della sicurezza dei sistemi informativi (Chief Information Security Officer, CISO) e del responsabile IT.

Il processo di gestione del rischio privacy

Prima di effettuare una DPIA sarà allora necessario impostare un processo di gestione del rischio privacy che comprenderà la stessa DPIA, ma che prevedrà alcune fasi preliminari per dimostrare l'accountability del titolare del trattamento e altre fasi successive alla stessa DPIA, essenziali per gestire correttamente le risultanze della valutazione, in modo da rendere l'intero processo adattabile e aggiornabile al mutare delle condizioni e delle esigenze organizzative.

A tal fine, il processo di gestione del rischio privacy è divisibile nelle seguenti fasi:

1. **Mappatura dei trattamenti effettuati dal titolare**, che tenga in debito conto della tipologia dei dati trattati, delle categorie di interessati, nonché delle finalità del trattamento;
2. **Valutazione del rischio privacy** sui trattamenti mappati in Fase 1, tenendo conto del contesto del trattamento e delle tecnologie sottostanti;
3. **Conduzione della DPIA**, per i soli trattamenti individuati come potenzialmente rischiosi;
4. **Notifica al Garante dei trattamenti** risultati come ad alto rischio a seguito della DPIA;
5. **Registro dei rischi privacy**, al fine di mantenere un elenco aggiornato e periodicamente adattabile delle valutazioni effettuate, incluse le DPIA.

Analizziamole nel dettaglio.

Mappatura dei trattamenti: cos'è e come realizzarla

Per quanto riguarda la mappatura dei trattamenti, questa può coincidere con il registro dei trattamenti effettuato, se possibile, in fase di assessment, da personale qualificato. Un registro ben redatto, cioè sulla base dei criteri contenuti nell'art. 30 del GDPR, conterrà infatti le informazioni richieste dall'art.35 succitato, cioè le finalità del trattamento, una descrizione delle categorie di interessati e delle categorie di dati personali.

Inoltre, un **registro redatto conformemente al GDPR** sarà utilissimo anche nella seconda fase del processo (la valutazione del rischio che vedremo più avanti), poiché consentirà di avere già a disposizione delle informazioni relative al contesto aziendale sia interno sia esterno, ed altre informazioni utili alla valutazione del rischio: in particolare enumerando i responsabili del trattamento, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate, nonché i termini ultimi previsti per la cancellazione delle diverse categorie di dati e la descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del GDPR.

Valutazione del rischio: i criteri per effettuarla

L'attività dovrebbe iniziare stabilendo cosa si intende per "rischio" rispetto all'organizzazione oggetto della valutazione. A tal fine è possibile utilizzare, ad esempio, la nota ISO/IEC 27000, dove **per "rischio" si intende un effetto dell'incertezza sugli obiettivi**, interpretando "l'effetto" nella sua accezione negativa, oppure le linee guida concernenti la valutazione di impatto sulla protezione dei dati del WP29 (Working Party 29), dove per "rischio" si intende uno scenario descrittivo di un evento e delle relative conseguenze che sono stimate

in termini di gravità e probabilità. La "gestione del rischio", quindi, è definibile come l'insieme coordinato delle attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio.

Il rischio, in riferimento ai "diritti e le libertà" degli interessati, va inteso come relativo al diritto alla privacy, ma può riguardare anche altri diritti fondamentali quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione. Tali diritti saranno più o meno a rischio in base al trattamento effettuato in relazione alla realtà organizzativa cui la valutazione si applica e le finalità e modalità di trattamento utilizzate; pertanto il titolare del trattamento dovrebbe andare oltre i nove criteri (o esempi generali) elencati dal WP29 nelle Linee guida sulla DPIA (WP248), poiché se da un lato è vero che quanto maggiore è il numero dei criteri soddisfatti, tanto maggiore sarà la necessità di effettuare una DPIA, dall'altro i criteri stessi non tengono in considerazione gli aspetti legati alla sicurezza informatica, pur rappresentando una fonte di rischio ulteriore per i diritti e le libertà dell'interessato.

A tal fine, **occorrerà integrare i criteri "privacy" con dei criteri di sicurezza del trattamento**, partendo dall'assunto che la sicurezza dello stesso prevede la capacità di un'organizzazione di saper rispondere a determinati eventi tali per cui il dato (personale) gestito sarà tutelato rispettando i **parametri cosiddetti RID, cioè Riservatezza, Integrità e Disponibilità**, rispettivamente, in termini di divulgazione/accesso strettamente controllato, inalterabilità e continua disponibilità.

La valutazione preliminare di rischio dovrebbe allora contenere almeno i seguenti criteri:

Criteri Privacy:

1. Trattamenti valutativi o di scoring (incluso profilazione), poiché possono incidere sulla vita dell'interessato e condizionarne il comportamento o le scelte future;
2. Decisioni automatizzate con "effetti giuridici sulla persona fisica" ovvero che "incidono in modo analogo significativamente su dette persone fisiche" (art. 35, paragrafo 3, lettera a);
3. Monitoraggio sistematico, poiché può avvenire in circostanze tali da non consentire agli interessati di comprendere chi vi stia procedendo, per quali finalità o sottrarsi al trattamento;
4. Dati sensibili o dati di natura estremamente personale, in particolare poiché una loro violazione (il cosiddetto data breach) comporta un grave impatto sulla vita dell'interessato;
5. Trattamenti di dati su larga scala, per numero di soggetti interessati, volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento, durata, o persistenza, dell'attività di trattamento e ambito geografico dell'attività di trattamento;
6. Combinazione o raffronto di insiemi di dati, poiché potrebbero comportare trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
7. Dati relativi a interessati vulnerabili (incluso minori e lavoratori) poiché è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento;
8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative, poiché può generare forme innovative di raccolta e utilizzo dei dati;
9. Tutti quei trattamenti che, di per sé, "impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto" (art. 22 e considerando 91), come ad esempio i trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o la stipulazione di un contratto.

Criteri Security:

1. Analisi del contesto organizzativo, sia interno sia esterno con particolare attenzione alle persone cosiddette “chiave” e partner strategici (incluso i fornitori);
2. Mappatura degli asset, cioè degli strumenti aziendali utilizzati (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei), con particolare riferimento agli archivi e server, soprattutto se in outsourcing;
3. Identificazione delle possibili minacce, cioè delle cause potenziali di un incidente che possono comportare danni ad un sistema o all’organizzazione, come ad esempio persone malintenzionate e non, strumenti tecnici ed eventi naturali;
4. Analisi delle vulnerabilità, mediante, ad esempio, test effettuati e relative relazioni, inclusi i remediation plan stabiliti;
5. Misure di sicurezza (idonee) implementate dall’organizzazione.

È utile ricordare che la semplice circostanza per cui non siano soddisfatte le condizioni che generano un obbligo di condurre la DPIA non riduce l’obbligo per il titolare del trattamento di mettere in atto misure finalizzate a gestire in modo idoneo i rischi per i diritti e le libertà degli interessati. Questo si traduce, nella pratica, con l’adozione comunque di un processo valutativo continuo, sì da monitorare i rischi inerenti i trattamenti effettuati ed individuare, anche in un secondo momento, l’occorrenza, per un determinata tipologia di trattamenti, del rischio elevato per i diritti e le libertà delle persone fisiche.

Procedere ad una DPIA: linee guida e aspetti chiave

Condurre una valutazione d’impatto privacy è un’analisi che trova i suoi fondamentali all’interno del Regolamento (GDPR) all’art. 35, paragrafo 7, e nei considerando 84 e 90. Sempre il Regolamento aggiunge che il **rispetto di un codice di condotta** (ai sensi dell’art. 40) come elemento probante le scelte effettuate deve essere tenuto in considerazione (ex art. 35, paragrafo 8) nel valutare l’impatto di un trattamento, purché il codice di condotta sia idoneo con riguardo allo specifico trattamento Allo stesso tempo, è promossa l’utilità di strumenti alternativi come supporto, ma assolutamente non sostitutivi, quali eventuali certificazioni, sigilli e marchi finalizzati a dimostrare che determinati trattamenti da parte di titolari e responsabili rispettano il Regolamento (art. 42) nonché le norme vincolanti d’impresa (BCR).

La DPIA deve essere effettuata a monte del trattamento, cioè in fase di progettazione e deve essere aggiornata con regolarità, attraverso la ripetizione, ad esempio, di singole tappe della valutazione, poiché la scelta di determinate misure tecniche o organizzative potrà non più essere valida nel caso di un mutato contesto organizzativo.

Spetta al titolare del trattamento garantire l’effettuazione della DPIA (art. 35, paragrafo 2anche se la conduzione materiale della DPIA può essere affidata ad un soggetto esterno. Nel caso sia presente un Responsabile della Protezione dei Dati (RPD/DPO), questi avrà un ruolo consultivo e di monitoraggio nello svolgimento della DPIA (art. 39, paragrafo 1, lettera c, del GDPR). Nel caso il trattamento sia affidato ad un soggetto esterno all’organizzazione, cioè ad un responsabile del trattamento, quest’ultimo deve assistere il titolare nella conduzione della DPIA, fornendo ogni informazione necessaria conformemente all’art. 28, paragrafo 3, lettera f, del GDPR.

Il titolare del trattamento dovrà inoltre scegliere se raccogliere le opinioni degli interessati o dei loro rappresentanti (art. 35, paragrafo 9, del GDPR), ad esempio attraverso questionari, e motivare, nel caso, se la decisione assunta si discosta dall’opinione degli stessi. Al contrario, il titolare dovrebbe documentare le

motivazioni della mancata consultazione degli interessati, ad esempio perché potrebbe pregiudicare la riservatezza dei piani aziendali o essere impraticabile.

Sarà in ogni caso importante definire e documentare eventuali ulteriori ruoli e responsabilità in rapporto alle politiche, ai processi e alle disposizioni interne all'organismo, quali, ad esempio: consultare il responsabile della sicurezza dei sistemi informativi (Chief Information Security Officer, CISO) ove designato, o più in generale esperti indipendenti provenienti da diversi ambiti disciplinari (legale, tecnologico, sicurezza, sociologico, etico ecc.).

Una DPIA dovrà quindi contenere:

1. Una descrizione sistematica e funzionale del trattamento;
2. Gli strumenti coinvolti nel trattamento dei dati personali;
3. I codici di condotta a cui l'Organizzazione ha deciso di aderire;
4. Una valutazione di necessità e proporzionalità del trattamento, incluse le misure adottate;
5. Una valutazione delle minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilità dei dati, incluse relative probabilità e gravità;
6. Una stima degli impatti potenziali sui diritti e le libertà degli interessati in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilità dei dati;
7. Le misure per la gestione dei rischi e mitigazione degli impatti;
8. Il coinvolgimento dei soggetti interessati e opinione del RPD/DPO.

Emerge chiaramente come per il punto I la fase 1 del processo (Mappatura dei trattamenti) tornerà di immediata utilità, e per i punti V-VIII la fase 2 (Valutazione del rischio) del processo risulterà sinergica e quindi funzionale allo schema stesso della DPIA.

Come effettuare materialmente una DPIA risulterà, infine, una scelta assolutamente soggettiva da parte del titolare del trattamento, che potrà utilizzare strumenti comuni come dei fogli di calcolo, adattabili e aggiornabili con estrema semplicità, soprattutto in relazione alle informazioni da gestire ed elaborare, oppure utilizzare dei software specifici, tenendo bene a mente il limite intrinseco degli stessi: sono concepiti per essere utilizzabili da tutti e di conseguenza, possono trascurare le particolarità dei singoli ed il contesto in cui operano.

A tal proposito, sul sito del Garante italiano si fa riferimento al software PIA del CNIL, inserendo l'importante disclaimer sull'inapplicabilità dello stesso ad ogni situazione di trattamento, essendo stato concepito soprattutto come ausilio metodologico per le PMI, e quindi, di far riferimento ad esso come un utile supporto di orientamento allo svolgimento di una DPIA. Integrando, ad esempio, lo schema proposto dal CNIL con i parametri elencati in fase 2 (Valutazione del rischio) e le relative risultanze, si disporrà di uno schema pragmatico in grado di analizzare, in maniera ragionevole, il rischio complessivo che il trattamento previsto può comportare per i diritti e le libertà degli interessati, alla luce dello specifico contesto.

La notifica al Garante in caso di violazione dei dati

A conclusione della DPIA, il titolare dovrà **decidere quali saranno le misure più idonee per attenuare i rischi emersi**, riportandoli ad un livello "accettabile". Nel corso della fase 2 del processo (Valutazione del rischio) il titolare avrà disposto, o almeno individuato e pianificato i rimedi necessari per gestire il rischio che incombe sui dati personali e attenuarli, dimostrando l'osservanza del regolamento per procedere al trattamento senza consultare l'autorità di controllo.

Nel caso in cui, però, i rischi individuati permangano, anche a seguito di misure/rimedi specifici, e il loro livello rimane "non accettabile" il titolare dovrà consultare l'autorità di controllo, avviando un iter di valutazione da parte dell'autorità competente che, nei fatti, è paragonabile alla procedura di verifica preliminare prevista dal vecchio codice.

Il WP29 riporta un esempio del cosiddetto **rischio residuale elevato**, non accettabile, in particolare descrivendo la situazione generica derivante dall'impossibilità di ridurre il numero di soggetti in grado di accedere ai dati in ragione delle modalità di condivisione, utilizzo o distribuzione dei dati – si pensi ai servizi in cloud, soprattutto su base gratuita – e le conseguenze derivanti per l'interessato (significative, irreversibili e non eliminabili) come la minaccia per la vita dello stesso, la perdita o sospensione del rapporto lavorativo, nonché danni di natura finanziaria.

Registro delle DPIA: ecco di cosa si tratta

Sia nel caso di DPIA i cui risultati siano una notifica al Garante o meno, sia nei casi in cui, a giudizio del titolare, il trattamento non rappresenta un rischio elevato per i diritti e le libertà degli interessati, **il titolare è obbligato a motivare e documentare le scelte effettuate**. In particolare, il titolare sarà obbligato a dimostrare l'eventuale mancata conduzione della DPIA, allegando o annotando l'opinione del Responsabile della Protezione dei Dati. Pertanto, impostare e condurre con particolare attenzione la fase 2 del processo (Valutazione del rischio) tornerà nuovamente di estrema utilità.

Nella pratica, **il registro delle DPIA si traduce nella redazione e nel mantenimento di un registro apposito** (un foglio di calcolo è ampiamente sufficiente ed elastico alle modifiche) o **nella integrazione del registro dei trattamenti** svolti sotto la propria responsabilità delle informazioni suddette, divenendo un vero e proprio strumento di controllo per il titolare e per il DPO, in cui emergono sia la mappatura delle attività di trattamento effettuate sia la valutazione del rischio annesso e l'eventuale pianificazione delle misure necessarie per mitigare rischi e impatti.

Conclusioni

Per concludere, il processo di valutazione dei rischi privacy in azienda si esplica attraverso una serie di attività che riguardano aspetti privacy e di sicurezza che andranno analizzati contestualmente. Tutti gli elementi che lo compongono, se ben identificati ed analizzati, costituiranno la traccia per realizzare una valutazione pertinente ed efficiente, adattabile ad ogni contesto ed in grado di indicare al titolare del trattamento se sia necessario procedere con la notifica al Garante o assumersi la responsabilità di procedere al trattamento.