Cooperazione Trentina

inFederazione

Valutazione d'impatto sulla protezione dei dati personali (DPIA)

2023

Punto d'approdo

società cooperativa sociale

Indice

Introduzione alla DPIA

Cos'è la DPIA

La DPIA è una procedura prevista dall'articolo 35 del Regolamento UE 2016/679 (GDPR) finalizzata a descrivere un trattamento di dati, valutarne la necessità, la proporzionalità e i rischi per i diritti e le libertà delle persone fisiche che possano derivarne.

In base al principio di responsabilizzazione del titolare del trattamento, la DPIA sostituisce l'obbligatorietà di notifica del trattamento dei dati personali alle Autorità di controllo, prevista dalla normativa antecedente al Regolamento.

Con l'introduzione della DPIA, il GDPR rende evidente che ai fini dell'elaborazione di un sistema di sicurezza nel trattamento dei dati personali non sempre basta l'analisi dei rischi e la predisposizione di misure adeguate. In alcuni casi è necessario documentare di aver valutato l'impatto sulla protezione dei dati, da cui dipende la protezione del diritto alla riservatezza delle persone fisiche.

Il Regolamento impone, all'art.24, l'analisi dei rischi che un trattamento comporta al fine di mettere in atto tutte le misure tecniche e organizzative adeguate a rendere tale trattamento conforme alle norme del Regolamento. All'art. 35, invece, prevede una specifica valutazione di impatto quando i trattamenti, considerate le circostanze indicate nella norma, possono presentare "*un rischio elevato per i diritti e le libertà delle persone fisiche*".

La DPIA è richiesta in diversi specifici casi, previsti in un elenco non esaustivo dallo stesso GDPR (art. 35, co. 3) e che è stato integrato dal Gruppo di Lavoro Articolo 29 nel documento WP 248 rev.01 dell'ottobre 2017 e dal Garante per la Protezione dei Dati Personali con apposito provvedimento dell'ottobre 2018.

Contenuto della DPIA

In base a quanto stabilito dall'art. 35 GDPR co.7, la valutazione di impatto contiene almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, se del caso, l'interesse legittimo dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- 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 Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il titolare del trattamento deve effettuare un monitoraggio costante dei trattamenti in relazione ad eventuali variazioni del rischio per la tutela del dato personale. Nel caso in cui, in seguito alla DPIA, risulti che il rischio non possa essere ridotto attraverso l'utilizzo delle tecnologie e per gli elevati costi

di attuazione, prima di effettuare il trattamento occorre chiedere una consultazione all'Autorità di controllo.

Per quanto riguarda il concetto di "rischio", secondo il Gruppo di Lavoro Articolo 29 "*per rischio si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità*" per i diritti e le libertà degli interessati. Nello specifico, un rischio privacy mette a repentaglio la riservatezza, l'integrità e la disponibilità dei dati personali trattati.

Di conseguenza, il presente documento elenca le minacce che incombono sui dati personali dei soggetti coinvolti nei processi di trattamento oggetto della DPIA, valutando la probabilità e la gravità dei conseguenti rischi per i diritti e le libertà di tali soggetti, nel rispetto delle indicazioni del considerando 90, a mente del quale "*è opportuno che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio*".

Campo di applicazione

L'art.35 GDPR, come già ricordato, impone di svolgere una valutazione d'impatto sulla protezione dei dati nel caso in cui un tipo di trattamento possa presentare "*un rischio elevato per i diritti e le libertà delle persone fisiche*".

Il decreto legislativo n.24 del 10 marzo 2023, attuativo della direttiva UE 2019/1937, regola la materia del c.d. whistleblowing, imponendo agli enti privati aventi determinate caratteristiche di attivare di un canale di segnalazione interno che consenta a dei soggetti qualificati di segnalare "*comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato*" (art. 2 d. lgs. 24/2023) dei quali il soggetto segnalante venga a conoscenza nell'ambito del proprio contesto lavorativo.

E' evidente che il trattamento di dati personali conseguente all'attivazione del canale è suscettibile di integrare, per il soggetto segnalante e per gli altri interessati menzionati nella segnalazione, il rischio menzionato dall'art. 35 GDPR. Lo stesso decreto legislativo 24, infatti, impone ai soggetti gestori del canale interno di segnalazione di effettuare una valutazione d'impatto sulla protezione dei dati (art. 13, co 6). In questo modo, il titolare del trattamento individua le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati.

Punto d'approdo s.c., in ossequio a quanto previsto dall'art. 4 del decreto, ha stipulato un contratto con Federazione Trentina della Cooperazione per la messa a disposizione di una piattaforma informatica per le segnalazioni e per la gestione delle segnalazioni ricevute.

I trattamenti da sottoporre alla valutazione d'impatto, dunque, sono i seguenti:

- Gestione delle segnalazioni whistleblowing

Metodologia applicata

La valutazione d'impatto viene effettuata sulla scorta delle indicazioni contenute nell'*Handbook on security of personal data processing* pubblicato da ENISA e nelle *Linee Guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare rischio elevato" ai fini del Regolamento UE 2016/679* del Working Party 29.

Citando proprio da quest'ultimo documento, "[...] *Il considerando 90 del regolamento generale sulla protezione dei dati delinea una serie di elementi costituivi della valutazione d'impatto sulla protezione dei dati che si sovrappone a elementi ben definiti della gestione del rischio (ad esempio norma ISO 3100026). In termini di gestione dei rischi, una valutazione d'impatto sulla protezione dei dati mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche, utilizzando i seguenti processi:*

- *stabilendo il contesto: "tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio";*
- *valutando i rischi: "valutare la particolare probabilità e gravità del rischio";*
- *trattando i rischi: "attenuando tale rischio" e "assicurando la protezione dei dati personali", e "dimostrando la conformità al presente regolamento".*

Lo svolgimento della DPIA, dunque, segue il seguente iter:

A) Definizione dell'operazione di trattamento e del suo contesto – comprende la descrizione delle caratteristiche principali delle operazioni di trattamento e le valutazioni in ordine alla necessità e alla proporzionalità del trattamento;

B) Comprensione e valutazione dell'impatto – sulla base di quanto emerso al punto a), viene effettuata una valutazione dell'impatto sui diritti e sulle libertà fondamentali delle persone fisiche derivanti dalla possibile perdita di riservatezza, integrità e disponibilità (c.d. RID) dei dati personali. In particolare, sarà necessario definire il livello dell'impatto della perdita di ciascuno dei tre elementi della RID. I livelli d'impatto attribuibili sono i seguenti:

LIVELLO D'IMPATTO	DESCRIZIONE
Irrilevante = 1	Gli interessati non incontrano inconvenienti significativi
Basso = 2	Gli interessati possono incontrare disagi minori, che supereranno senza alcun problema (perdita di tempo, fastidio)
Medio = 3	Gli interessati possono incontrare significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso a servizi, stress)
Alto = 4	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (perdite finanziarie, limitazione dei diritti, perdita di riservatezza dei dati personali, perdita del controllo dei dati personali, limitazione dei diritti)
Molto Alto = 5	Gli interessati possono subire conseguenze significative o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.)

L'impatto complessivo sarà dato dal maggiore tra l'impatto per perdita di riservatezza, l'impatto per perdita di integrità e quello per perdita di disponibilità.

C) Definizione di possibili minacce e valutazione della loro probabilità – lo scopo di questa fase è comprendere le minacce correlate al contesto e valutare la loro probabilità di occorrenza. ENISA, nel documento sopra citato, ha definito una serie di domande di valutazione, relative a diversi ambienti di elaborazione e trattamento dei dati (risorse di rete e tecniche; processi/procedure relativi alle operazioni di trattamento dati; diverse parti e persone coinvolte nelle operazioni di trattamento; settore di operatività e scala del trattamento).

D) Valutazione del rischio e conseguente selezione delle misure di sicurezza necessarie

DPIA – Operazione di trattamento e contesto (STEP 1)

Descrizione del trattamento

Titolare del trattamento: Punto d'approdo s.c.s.

Responsabili del trattamento: Federazione Trentina della Cooperazione

Sub-Responsabili del trattamento: Whistleblowing Solutions I.S. s.r.l.

Autorizzati al trattamento: OdV della cooperativa

Finalità del trattamento: gestione delle segnalazioni whistleblowing

Processo di trattamento dati personali: presa in carico la segnalazione; verifica della rilevanza della segnalazione ai sensi di quanto previsto dalla disciplina in materia di whistleblowing; classificazione della segnalazione; raccolta di documentazione, informazioni o altro materiale necessario per valutare la segnalazione; eventuale interlocuzione con il soggetto segnalante e/o con altri soggetti coinvolti; riscontro al segnalante; chiusura la segnalazione.

Interessati: soggetto segnalante; soggetti che vengono segnalati; soggetti indicati nella segnalazione.

Categorie dei dati trattati: dati personali comuni; dati personali appartenenti a particolari categorie; dati relativi a condanne penali e reati.

Come vengono trattati i dati personali: la segnalazione viene inoltrata attraverso l'utilizzo la piattaforma informatica Whistleblowing – Cooperazione Trentina (da ora in avanti anche Piattaforma), sviluppata da un fornitore esterno (Whistleblowing Solutions I.S. s.r.l.). L'accesso alla Piattaforma è consentito solamente al personale del soggetto gestore tramite credenziali personali. Al momento della segnalazione, al soggetto che la effettua viene rilasciato un codice numerico (noto solamente a lui) con il quale potrà verificare lo stato della segnalazione e le eventuali interlocuzioni con il gestore. Le segnalazioni, a scelta di chi le effettua, possono essere inviate in forma anonima o fornendo i dati identificativi, secondo quanto previsto dalla normativa.

Il personale del soggetto gestore, specificamente autorizzato e formato in materia, gestisce la segnalazione garantendo la riservatezza del suo contenuto e dell'identità del soggetto segnalante dal momento della ricezione a quello della chiusura. I dati personali non necessari alla gestione della segnalazione vengono immediatamente cancellati.

Punto d'approdo s.c. si è dotata di un'apposita procedura di gestione delle segnalazioni, che viene seguita pedissequamente.

Soggetti esterni che possono venire a conoscenza dei dati: nessuno.

Periodo di conservazione dei dati: per il tempo necessario al trattamento della segnalazione e, comunque, non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione

Sistemi di trattamento: piattaforma informatica Whistleblowing – Cooperazione Trentina; supporti

cartacei (solo se strettamente necessario)

Misure di sicurezza presenti

TITOLARE – Punto d'approdo s.c.

Misure del titolare per garantire i diritti dell'interessato: informativa sul trattamento dei dati personali; procedure interne all'organizzazione per effettuare la segnalazione; contrattualizzazione e accordo sul trattamento dei dati personali con un fornitore adeguato dal punto di vista privacy; regolamento interno per il trattamento di dati personali.

RESPONSABILE – Federazione Trentina della Cooperazione

Misure del responsabile per garantire i diritti dell'interessato: autorizzazione al trattamento per i soggetti che gestiscono le segnalazioni; formazione dei soggetti che gestiscono le segnalazioni; procedura per la gestione di una violazione di dati, regolamento interno per il trattamento di dati personali.

SUB-RESPONSABILE - Whistleblowing Solutions s.r.l.

Misure di Riservatezza applicate dal sub-responsabile (Misure per prevenire accesso illegittimo): ogni macchina virtuale implementa configurazione securizzata con Full Disk Encryption, SecureBoot, Apparmor, Iptables; connessioni protette tramite protocollo TLS 1.2+; connessioni amministrative privilegiate mediate tramite accesso VPN; firewall perimetrale; segregazione della rete in molteplici VLAN; computer dotati di antivirus e firewall; personale formato.

Misure di Integrità applicate dal sub-responsabile (Misure per prevenire modifica indesiderata): firewall perimetrale; accessi separati per utenti diversi; VPN; audit di sicurezza periodici e non periodici; sicurezza fisica dei locali dei datacenter; connessioni amministrative privilegiate mediate tramite accesso VPN; ogni macchina virtuale vede esposizione di rete limitata all'effettiva necessità; computer dotati di antivirus e firewall; personale formato.

Misure di Disponibilità applicate dal sub-responsabile (Misure per prevenire scomparsa dei dati): entrambi i server fisici eseguono una macchina virtuale di Key Menagement System (KMS) per consentire continuità di servizio con immediato automatico riavvio dei sistemi senza intervento amministrativo anche in caso di totale fallimento di uno dei due server fisici; backup remoto giornaliero con data retention di 7 giorni per finalità di disaster recovery; ogni macchina virtuale vede esposizione di rete limitata all'effettiva necessità

Misure di Riservatezza, Integrità e Disponibilità applicate dalla Piattaforma: utilizzo di uno specifico protocollo crittografico (le cui caratteristiche sono descritte nell'allegato 1); policy di sicurezza password e autenticazione a due fattori; connessioni amministrative privilegiate mediate tramite accesso VPN; sistema di audit log sicuro e in linea con le necessità di confidenzialità richieste dalla normativa in materia di whistleblowing; log delle attività del segnalante privi delle informazioni identificative del segnalante; audit di sicurezza periodici e non periodici; sicurezza fisica dei locali dei datacenter; datacenter fornitore IaaS certificati ISO 27001; firewall perimetrale; accessi separati per utenti diversi; sistemi soggetti a backup remoto giornaliero con policy di data retention di 7 giorni; manutenzione periodica e accessibile solamente al personale di Whistleblowing Solutions; connessioni protette tramite protocollo TLS 1.2+; datacenter del fornitore IaaS dotati di struttura di controlli accessi, monitoraggio 24/7, videosorveglianza, sistema di allarme e presidio 24/7; datacenter fornitore IaaS certificati ISO 27001.

Per il dettaglio delle misure di sicurezza presenti si rinvia al documento tecnico fornito dal fornitore della piattaforma (allegato 7.1 al Vademecum).

Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità

Nel caso in esame, si può presumere che la necessità e la proporzionalità dei trattamenti siano da considerarsi de facto esistenti, in quanto la gestione delle segnalazioni whistleblowing è prevista dalla legge.

In ogni caso, si segnala che i trattamenti oggetto della valutazione presentano inoltre tutte le caratteristiche che, secondo il WP 29, garantiscono il rispetto dei principi di necessità e proporzionalità:

- uso di dati adeguati, rilevanti e limitati: i dati personali non utili al trattamento di una segnalazione vengono subito cancellati, in ossequio al principio di minimizzazione e a quanto previsto dall'art. 13, co. 2 d. lgs. 24/2023. In ogni fase della gestione della segnalazione vengono richiesti ulteriori dati personali solamente se strettamente necessari per dare adeguato seguito a quanto segnalato;
- finalità specifiche, legittime e determinate: il trattamento viene effettuato per la finalità prevista dalla normativa (gestione delle segnalazioni), come tale legittima e precisamente determinata. Non vengono perseguite ulteriori finalità da parte del soggetto gestore;
- liceità dei trattamenti: il trattamento è fondato su adeguata base giuridica – obbligo di legge per i dati comuni, effettuazione del trattamento per motivi di interesse pubblico rilevante per i dati particolari;
- conservazione per un periodo limitato: la conservazione dei dati raccolti avverrà per il tempo necessario al trattamento della segnalazione da parte del soggetto gestore e comunque non oltre cinque anni dalla comunicazione dell'esito finale della procedura di segnalazione (come indicato dall'art. 14 del d. lgs. 24/2023).

DPIA – Comprensione e valutazione dell'impatto (STEP 2)

RID	DOMANDA	IMPATTO	
RISERVATEZZA	Si prega di riflettere sull'impatto che la perdita di riservatezza (es. divulgazione non autorizzata) dei dati personali – nel contesto in cui il Titolare del trattamento svolge la propria attività – potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza	☐ Irrilevante ☐ Basso ☐ Medio ☒ Alto ☐ Molto alto	4
INTEGRITA'	Si prega di riflettere sull'impatto che la perdita di integrità (es. alterazione non autorizzata) dei dati personali – nel contesto in cui il Titolare del trattamento svolge la propria attività – potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza	☐ Irrilevante ☐ Basso ☐ Medio ☒ Alto ☐ Molto alto	4
DISPONIBILITA'	Si prega di riflettere sull'impatto che la perdita di disponibilità (es. distruzione non autorizzata) dei dati personali – nel contesto in cui il Titolare del trattamento svolge la propria attività – potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza	☐ Irrilevante ☐ Basso ☐ Medio ☒ Alto ☐ Molto alto	4

Impatto complessivo
(Dato dal maggiore tra i tre impatti sopra indicati)

ALTO = 4

DPIA – Definizione di possibili minacce e valutazione della loro probabilità (STEP 3)

RISORSE DI RETE E TECNICHE		PROBABILITA'	
Qualche parte del trattamento viene eseguita tramite Internet?	Si	Basso	1
È possibile fornire l'accesso a un sistema interno tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?	No		
Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	No		
Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	No		
Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?	No		
PROCESSI/PROCEDURE RELATIVI ALLE OPERAZIONI DI TRATTAMENTO DEI DATI		**PROBABILITA'**	
I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	No	Basso	1
L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	No		
I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	No		
I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	No		
Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	No		
PARTI/PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI		**PROBABILITA'**	
Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	No	Basso	1
Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore/terza parte (responsabile del trattamento)?	Si		
Gli obblighi delle parti/persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	No		
Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	No		
Le persone/le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e/o distruggere in modo sicuro i dati personali?	No		
SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO		**PROBABILITA'**	
Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	Si	Basso	1
La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	no		
Hai ricevuto notifiche e/o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno	No		
Un'operazione di elaborazione riguarda un grande volume di individui e/o dati personali?	No		
Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	No		
		Tot.	4

Basso (1)
Medio (2)
Alto (3)

LIVELLO DI PROBABILITA' TOTALE DELLE MINACCE: BASSO (1)

DPIA – Misurazione del rischio (STEP 4)

Riconosciuta la necessità di effettuare una valutazione d'impatto, descritti nel dettaglio i trattamenti che devono essere oggetto di tale valutazione, delineati i sistemi di misura della probabilità e della gravità del rischio, abbiamo riassunto i risultati della valutazione d'impatto nella tabella sottostante.

MISURA DEL RISCHIO		IMPATTO				
		Molto basso	Basso	Medio	Alto	Molto alto
PROBABILITA'	Basso	1	2	3	4	5
	Medio	2	4	6	8	10
	Alto	3	6	9	12	15

Sulla base del risultato è possibile ottenere i seguenti scenari

RISCHIO ACCETTABILE: Il Titolare gestisce il rischio attraverso le misure organizzative e tecnologiche esistenti.

RISCHIO PARZIALMENTE ACCETTABILE: il Titolare deve ottimizzare le misure organizzative e tecnologiche esistenti con alcune attività preventive e di miglioramento.

RISCHIO NON ACCETABILE: il Titolare deve predisporre un piano di misure di sicurezza più elevate al fine di gestire il rischio, con un piano di monitoraggio costante delle misure intraprese. Il titolare deve eventualmente fare ricorso alla consultazione preventiva ex art.36 del GDPR.

La valutazione effettuata mostra che **i trattamenti in oggetto comportano un rischio accettabile per gli interessati**. Infatti:

Rischio finale = 4 (Impatto 4 x Probabilità 1)

Anche se i rischi per le libertà e i diritti degli interessati sono adeguatamente presidiati e mitigati, si raccomanda di mantenere costante il controllo sui processi oggetto del presente documento, poiché il mutare dei mezzi, dei soggetti o delle finalità del trattamento oppure delle misure di sicurezza predisposte dal titolare può avere effetti anche sulla valutazione d'impatto. La DPIA, infatti, è un documento dinamico.

Lo stesso GDPR, all'art. 35 co.11, afferma che "*se necessario, il titolare del trattamento 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*".

Muovendo da questa previsione, il Garante per la protezione dei dati personali ha sottolineato che "*dovrebbe comunque essere previsto un riesame continuo della DPIA, ripetendo la valutazione a intervalli regolari*".

Date le caratteristiche dei trattamenti e dei conseguenti rischi, si ritiene che il presente documento abbia validità annuale.