2025

Valutazione d’impatto sulla protezione dei dati (ex Art. 35 GDPR)

WHISTLEBLOWING

TEAM DPO

morolabs

Sommario

Introduzione 3
Campo di applicazione 3
Scopo 3
Destinatari 3
Normativa di riferimento 3
Che cosa è la PIA/DPIA (fonte WP248) 3
Cosa prevede il Regolamento per la PIA/DPIA (fonte WP248) 4
Quando è necessaria la DPIA 5
Modalità 7
Fasi PIA/DPIA 7
Fase 1: Elencare e raggruppare le attività di trattamento dei dati 7
Fase 2: Rispondere al questionario di valutazione dei valori soglia 8
Fase 4: Rispondere al questionario sulla PIA/DPIA 8
Fase 5: Identificare i rischi principali per la sicurezza 8
Fase 6: Come mitigare i rischi 8
Fase 7: Registrare l'implementazione 9
Consultazioni con l'Autorità di controllo 9
Revisione periodica PIA/DPIA 9
SCHEDA DPIA RELATIVA AL TRATTAMENTO 10

Introduzione

La Valutazione d'impatto sulla protezione dei dati o DPIA è un procedimento obbligatorio ai sensi del Regolamento (UE) 2016/679 quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate, a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori.

Lo strumento è coerente con il principio della responsabilizzazione o *accountability* introdotto dal GDPR al comma 2, Art. 5. Il Titolare è chiamato non solo a rispettare le norme del Regolamento ma anche all' attestazione formale dell'adozione delle misure (non più minime ma) idonee a garantire il rispetto di tali prescrizioni. La DPIA è quindi una procedura che permette la valutazione e soprattutto la dimostrazione della conformità alle norme in materia di protezione dei dati personali.

Campo di applicazione

Il campo di applicazione della presente Valutazione d'Impatto sulla Protezione dei Dati (PIA/DPIA) è relativo alla gestione del Whistleblowing, ai sensi del D.lgs. n. 24/2023.

Scopo

Ai sensi dell'art. 35 del Regolamento (UE) 2016/679 la PIA/DPIA è effettuata ogniqualvolta *un trattamento, allorché prevede in particolare l'uso di nuove tecnologie* (come nel caso di specie)*, 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*.

Destinatari

Destinatari di questo documento sono la Direzione, il Responsabile della Protezione dei Dati e il Gruppo di progetto GDPR; nei casi previsti, l'Autorità Garante può richiederne l'ostensione.

Normativa di riferimento

- Regolamento (UE) 2016/679 o GDPR - Articolo 35
- GDPR considerando 75, 84, 89, 90, 91, 92, 93
- WP 248 - Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "*possa presentare un rischio elevato*" ai sensi del Regolamento 2016/679
- Disposizioni e prescrizioni dell'Autorità Garante per la protezione dei dati personali

Che cosa è la PIA/DPIA (fonte WP248)

Una DPIA consiste in una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali (attraverso la valutazione di tali rischi e la definizione delle misure idonee ad affrontarli).

La DPIA è uno strumento importante in termini di responsabilizzazione (*accountability*) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del GDPR, ma anche a dimostrare l'adozione di misure idonee a garantire il rispetto di tali prescrizioni (art. 24 GDPR).

In altri termini, la DPIA è una procedura che permette di realizzare e dimostrare la conformità con le norme.

In base al Regolamento, l'inosservanza degli obblighi concernenti la DPIA può comportare sanzioni da parte della Autorità Garante della protezione dei dati personali. Il mancato svolgimento della DPIA quando il trattamento è soggetto a tale valutazione (art. 35, paragrafi 1 e 3-4), lo svolgimento non corretto di una DPIA (art. 35, paragrafi 2 e 7-9) o la mancata consultazione presso l'Autorità ove ciò sia necessario (art. 36, paragrafo 3, lettera e)) possono comportare sanzioni amministrative pecuniaria fino a un massimo di 10 milioni di Euro, ovvero – se si tratta di un'impresa – fino al 2% del fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore.

Cosa prevede il Regolamento per la PIA/DPIA (fonte WP248)

Il regolamento impone ai titolari di mettere in atto misure idonee a garantire ed essere in grado di dimostrare l'osservanza del Regolamento stesso, tenendo conto, fra gli altri, dei "*rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*" (art. 24, paragrafo 1). L'obbligo di condurre una DPIA, in determinate circostanze, deve essere collocato nel contesto del più generale obbligo imposto ai titolari di gestire correttamente i rischi connessi al trattamento di dati personali.

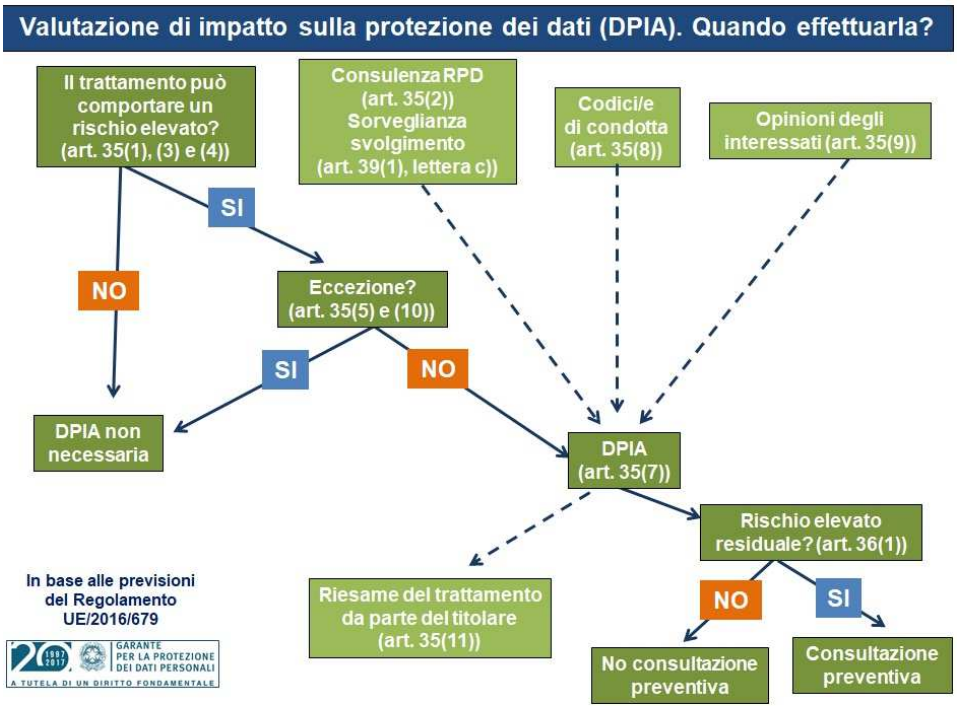
Per "rischio" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di probabilità e impatto (o gravità). La "gestione del rischio" è definita come l'insieme coordinato delle attività finalizzate a guidare e monitorare una organizzazione nei riguardi di tale rischio.

L'art. 35 del regolamento menziona la probabilità di un rischio elevato "per i diritti e le libertà delle persone fisiche".

Come già chiarito dal Gruppo di lavoro "Articolo 29" nella "Dichiarazione" sull'approccio basato sul rischio nel contesto giuridico della protezione dei dati, il riferimento ai "diritti e le libertà" degli interessati va inteso in primo luogo 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.

Coerentemente con l'approccio basato sul rischio che riforma il Regolamento rispetto alle normative precedenti, non è obbligatorio condurre una DPIA per ogni singolo trattamento. Viceversa, la DPIA è obbligatoria solo se una determinata tipologia di trattamenti *"può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"* (art. 35, paragrafo 1). Tuttavia, la semplice circostanza per cui non siano soddisfatte le condizioni che generano un obbligo di condurre la DPIA non riduce in alcun modo l'obbligo più generale cui sono sottoposti i titolari relativamente alla messa in atto di tutte le misure finalizzate a gestire in modo idoneo i rischi per i diritti e le libertà degli interessati. Nella pratica, ciò significa che i titolari devono valutare in modo continuativo i rischi connessi con i trattamenti, in modo da individuare le situazioni in cui una determinata tipologia di trattamenti "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche".*

La figura seguente illustra i principi fondamentali concernenti la DPIA in base al GDPR:



Quando è necessaria la DPIA

L'art. 35 del GDPR introduce l'obbligatorietà della Valutazione di impatto per i trattamenti che presentino rischi elevati per i diritti e le libertà delle persone fisiche, e in virtù della natura, l'oggetto, il contesto e le finalità dello stesso. Riuscire a identificare e discriminare caso per caso al fine di stabilire l'obbligatorietà o meno della valutazione non sempre risulta un'operazione semplice ed immediata, soprattutto se basata soltanto sulle basi previste dal Regolamento. Il Titolare, coadiuvato dal DPO, effettua una prevalutazione basandosi sulle informazioni essenziali già riportate nel Registro delle attività di trattamento al fine di valutare l'opportunità e/o la necessità di procedere o meno ad una DPIA.

Sempre l'art. 35 comma 3 riporta i casi per i quali si deve procedere tassativamente alla esecuzione della procedura di valutazione, ovvero:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Alcune tipologie di trattamenti effettuati rientrano immediatamente in una delle casistiche per cui non è necessario procedere con un approfondimento. Ma vi sono molte situazioni intermedie e particolarmente complesse che hanno spinto l'Autorità a illustrare in modo più specifico cosa rientra nell'obbligo.

Il chiarimento interpretativo dell'Autorità Garante riportato in Allegato 1 al Provvedimento n. 467 dell'11 ottobre 2018 [doc. web n. 9058979] (Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018) dove sono indicate le tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto, di seguito riportate:

1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad “aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato”.
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi).
3. Trattamenti che prevedono un utilizzo sistematico di dati per l’osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell’informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d’uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull’esercizio di un diritto fondamentale (quali i dati sull’ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell’interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5. Trattamenti effettuati nell’ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell’attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7. Trattamenti effettuati attraverso l’uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il Wi-Fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l’incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).
10. Trattamenti di categorie particolari di dati ai sensi dell’art. 9 oppure di dati relativi a condanne penali e a reati di cui all’art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell’attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell’attività di trattamento.

Altra doverosa considerazione, viste anche le dimensioni dell’Organizzazione, è la definizione di larga scala che, rispetto ai seguenti parametri:

a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
c. la durata, ovvero la persistenza, dell'attività di trattamento;

d. la portata geografica dell'attività di trattamento.

Modalità

Il regolamento fissa le caratteristiche basilari di una PIA/DPIA all'art. 35, paragrafo 7, e nei considerando 84 e 90:

- una descrizione [sistematica] dei trattamenti previsti e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per:
  - affrontare i rischi
  - dimostrare la conformità al regolamento.

La figura seguente illustra il processo iterativo generale relativo alla conduzione di una DPIA

Fasi PIA/DPIA

Fase 1: Elencare e raggruppare le attività di trattamento dei dati

Il Responsabile della Protezione dei Dati ha il compito di valutare quali trattamenti sottoporre alla procedura di PIA/DPIA in funzione della tipologia e soprattutto dei rischi per gli interessati.

Nel registro della Valutazione d'impatto sulla Protezione dei Dati sono inserite le registrazioni relative alle attività di analisi delle situazioni al fine di comprendere se è necessario o meno procedere con la consultazione presso l'Autorità Garante.

È possibile eseguire una singola valutazione contemporaneamente per diverse attività di trattamento dei dati, se tali attività di trattamento presentano rischi elevati simili. Il Responsabile della Protezione dei Dati decide quali attività di trattamento dei dati saranno valutate insieme.

Fase 2: Rispondere al questionario di valutazione dei valori soglia

Il Responsabile della Protezione dei Dati deve rispondere a tutte le domande per ciascuna attività di trattamento dei dati con l'aiuto di persone responsabili per ciascuna attività di trattamento dei dati.

Queste domande sono necessarie per determinare se un'attività di trattamento può comportare un rischio elevato per i diritti e le libertà delle persone fisiche.

Fase 3: Decidere se è necessaria la PIA/DPIA

Il Responsabile della Protezione dei Dati determinerà se un'attività di trattamento dei dati deve essere analizzata attraverso la valutazione dei seguenti aspetti:

1. Il trattamento prevede la raccolta, uso, conservazione o condivisione di dati sensibili dei residenti dell'Unione Europea?
2. Il trattamento prevede utilizza dati personali per prevedere preferenze personali, ubicazione movimento di persone, situazione finanziaria, salute o rendimento lavorativo dei residenti nell'Unione Europea?
3. Il trattamento aiuta a prendere decisioni che possono avere un impatto significativo sugli individui, come negazione del credito, rifiuto dei servizi, ecc.?
4. Il trattamento prevede comporta un monitoraggio sistematico degli spazi pubblici su larga scala?
5. Sono presenti altri rischi associati con il trattamento per i diritti e le libertà delle persone?

È sufficiente rispondere positivamente ad una sola delle risposte precedenti che risulta necessario procedere con la PIA/DPIA.

Anche se le risposte a tutte le domande nel questionario sono "No", il Responsabile della Protezione dei Dati può decidere di eseguire la Valutazione d'impatto sulla Protezione dei Dati se l'organizzazione ha bisogno di avere una visione più chiara dei rischi che incombono sui dati.

Fase 4: Rispondere al questionario sulla PIA/DPIA

Per ciascuna attività di trattamento dei dati in cui sia richiesta la Valutazione d'impatto sulla Protezione dei Dati, il Responsabile della Protezione dei Dati deve compilare il questionario sulla Valutazione d'Impatto sulla Protezione dei Dati nel Registro delle Valutazioni d'Impatto sulla Protezione dei Dati. Tutti gli elementi obbligatori devono essere inseriti.

Lo scopo di queste domande è ottenere una descrizione sistematica delle attività di redazione ed elaborazione.

Fase 5: Identificare i rischi principali per la sicurezza

Una volta che il Responsabile della Protezione dei Dati ha completato il questionario sulla Valutazione d'impatto sulla Protezione dei Dati, deve utilizzare i risultati per identificare ed elencare i principali rischi per la sicurezza associati all'attività di trattamento in questione.

In particolare, il Responsabile della Protezione dei Dati deve prendere in considerazione i rischi derivanti dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali.

Fase 6: Come mitigare i rischi

Una volta identificati ed elencati i rischi chiave, il Responsabile della Protezione dei Dati deve formulare un piano di mitigazione e inserirlo nel questionario. Le seguenti informazioni devono essere specificate:

- Misure protettive che devono essere implementate
- Responsabilità per l'implementazione
- Scadenze per l'implementazione

Fase 7: Registrare l'implementazione

Una volta implementata una protezione, il Responsabile della Protezione dei Dati deve registrarla nel questionario sulla Valutazione d'impatto sulla Protezione dei Dati sotto la colonna “Registrazione del Completamento”.

Consultazioni con l’Autorità di controllo

Se i risultati della Valutazione d'Impatto sulla Protezione dei Dati indicano che l’attività di trattamento dei dati può presentare un rischio elevato anche nel caso siano state implementate misure di sicurezza, il Responsabile della Protezione dei Dati procede con la consultazione presso l’Autorità di controllo prima dell’inizio del trattamento dei dati.

In questo caso, il Responsabile della Protezione dei Dati dovrà fornire all’Autorità di controllo le seguenti informazioni:

- Responsabilità del Titolare del trattamento, del contitolare (o contitolari) e del Responsabile
- Finalità e mezzi che saranno utilizzati per il trattamento
- Misure di sicurezza implementate per proteggere i dati
- Informazioni di contatto del Responsabile della Protezione dei Dati, e
- Risultati della Valutazione d'impatto sulla Protezione dei Dati

Revisione periodica PIA/DPIA

Il Responsabile della Protezione dei Dati deve riesaminare la PIA/DPIA in uno qualsiasi dei seguenti casi:

- Se i rischi relativi alle attività di trattamento dei dati sono modificati
- Se c’è un cambiamento significativo nelle attività di trattamento dei dati
- Se c'è un cambiamento nei requisiti legali
- Se un'azienda agisce come Responsabile e il Titolare richiede una revisione della PIA/DPIA

SCHEDA DPIA RELATIVA AL TRATTAMENTO

Informazioni generali del trattamento	
Denominazione del trattamento	**SEGNALAZIONI DI CONDOTTE ILLECITE (C.D. WHISTLEBLOWING)**
Trattamenti cui si riferisce	Protezione dei dati personali delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'Organizzazione, di cui siano venute a conoscenza nel contesto lavorativo nel quale operano, ai sensi del D.lgs. n. 24/2023 (c.d. *whistleblowing*).
Descrizione del trattamento	La segnalazione interna può essere effettuata con una delle seguenti modalità, in ottemperanza all'art. 4, co. 3, del D.lgs. 24/2023: a) in forma scritta, tramite **piattaforma informatica** disponibile sul portale web istituzionale della **Provincia di Ancona** al link https://amministrazionetrasparente.provincia.ancona.it/L190/?idSezione=54141 b) – raggiungibile dall'interno della sezione Amministrazione Trasparente, sottosezione "Altri Contenuti/Prevenzione della Corruzione". In esito all'inoltro della segnalazione, il sistema rilascia un codice identificativo da utilizzare per i successivi accessi al fine di monitorare lo stato di avanzamento dell'istruttoria. L'applicativo informatico utilizza un protocollo di crittografia che garantisce la tutela della riservatezza dell'identità del segnalante, della/e persona/e coinvolta/e, delle persone comunque menzionate nella segnalazione, nonché l'integrità e la non violabilità del contenuto della segnalazione e della documentazione ivi allegata; c) mediante un **incontro diretto**, su richiesta della persona segnalante, con il Responsabile della Prevenzione della Corruzione e della Trasparenza della **Provincia di Ancona**, debitamente verbalizzato previo consenso dell'interessato. I canali di segnalazione interna sono progettati in modo da consentire l'accesso alle segnalazioni solo da parte del personale espressamente autorizzato a trattare i dati inerenti alle medesime ai sensi degli artt. 28, 29 e 32, par. 4, del Regolamento (UE) 2016/679 e dell'art. 2-quaterdecies del D.lgs. 196/2003 ss.mm.ii.
Natura del trattamento	Registrazione, conservazione, consultazione, comunicazione, limitazione, cancellazione o distruzione.
Ambito di applicazione, contesto	Gestione delle segnalazioni – *Whistleblowing.*
Finalità del trattamento	Attività istituzionale.
Dati personali	Riferimenti segnalante e segnalati, eventuali notizie di violazioni.
Destinatari e autorizzati	Responsabile della Prevenzione della Corruzione e della Trasparenza della **Provincia di Ancona**.
Periodo di conservazione	Pari a 5 anni. Le segnalazioni interne e la relativa documentazione sono conservate 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.
Asset coinvolti (hardware, software, reti,	Piattaforma per la gestione informatizzata della segnalazione: https://amministrazionetrasparente.provincia.ancona.it/L190/?idSezione=54141

canali cartacei o di trasmissione cartacea)	
Codici di condotta adottati (arti. 35, par. 8)	N/A Non è al momento prevista l'adozione di specifici Codici di condotta.
Motivo della redazione della DPIA	Art. 35 par. 3 lett. a) e c) GDPR; Provvedimento dell'Autorità Garante n° 467/2018; Art. 13, comma 6 del D.lgs. 24/2023 prevede obbligatoriamente la DPIA; Rischio elevato per i diritti e le libertà degli interessati.
DPIA correlate / versioning	Prima redazione – v. 1.0
Valutazione delle misure atte a garantire necessità e proporzionalità del trattamento (art. 35, paragrafo 7, lettera b)	
Finalità determinate, esplicite e legittime	*Scopo*: facilitare la segnalazione garantendo al contempo il necessario livello di riservatezza al fine di tutelare il segnalante adottando tutte le misure tecniche e organizzative necessarie. *Trasparenza*: informativa privacy in forma breve (sulla piattaforma) e in forma più estesa pubblicata sul sito web istituzionale e reperibile nella regolamentazione specifica. *Precisazione della finalità*: espressa nell'informativa e DPIA pubblicata sul sito web istituzionale.
Liceità del trattamento (art. 6; art. 9 GDPR e art. 2-sexies D.lgs. 196/03)	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento: • Art. 6 par. 1 lettera c); • Art. 9 par. 2 lettera g); • Art. 13 del D.lgs. 24/2023.
Adeguatezza, pertinenza e non eccedenza (art. 5, par. 1, lettera c);	In conformità a quanto previsto dall'art. 13, comma 2 del D.lgs. 24/2023, i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente in conformità a quanto previsto dall'art. 13 del D.lgs. 24/2023. Nella form di acquisizione della segnalazione pubblicata in **piattaforma software** è utilizzato l'insieme minimo delle informazioni necessarie alle finalità della gestione delle segnalazioni stesse; in particolare, l'utente provvede ad inserire i dati utilizzando i campi disponibili come Nome, Cognome, Ruolo dell'utente che effettua la registrazione, i dati relativi all'ente (nome, indirizzo, CF e PI) ed eventualmente dei soggetti, interni o esterni, coinvolti nella segnalazione. La piattaforma software utilizzata permette di raccogliere le segnalazioni secondo i migliori questionari predisposti nell'ambito del *whistleblowing* messi a punto da "*Transparency International Italia*" in relazione alla normativa vigente in materia, ulteriormente ridotti nei campi obbligatori. Nel rispetto del principio del *privacy by design* tutti gli elementi della catena tecnologica utilizzati nella costituzione del sistema, quali l'applicativo software GlobaLeaks, i log di sistema e del firewall

	sono configurati per non registrare, o comunque mantenere registrati soltanto per pochi istanti, alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata. L'applicativo software GlobaLeaks vede abilitata oltre alla possibilità di navigazione anonima del browser senza accettazione di cookie, anche la navigazione tramite "*Tor Browser*" al fine di garantire un livello di anonimizzazione al passo con lo stato dell'arte della ricerca tecnologica in materia. Negli eventuali **incontri diretti** con il Responsabile della Prevenzione della Corruzione e della Trasparenza della **Provincia di Ancona** sono attuate accortezze similari durante la verbalizzazione.
Esattezza e aggiornamento dei dati (art. 5, par. 1, lettera d))	L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata. I dati personali possono essere tempestivamente cancellati o rettificati qualora, nel corso dell'istruttoria, risultassero inesatti rispetto alle finalità per le quali sono trattati («esattezza») in conformità a quanto previsto dall'art. 13 del D.lgs. 24/2023. Anche nel caso della segnalazione con incontro diretto l'esattezza e l'eventuale aggiornamento dei dati rimangono in campo al soggetto segnalante.
Limitazione della conservazione (*Retention*) (art. 5, par. 1, lettera e))	Le segnalazioni interne e la relativa documentazione sono conservate 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. Le segnalazioni scadute sono cancellate con procedura automatica in modalità sicura, non recuperabile.
Valutazione delle misure atte a garantire i diritti degli interessati[1]	
Informazioni fornite all'interessato (artt. 12, 13, 14)	Informativa sul sito web istituzionale in ottica stratificata e nella form iniziale di acquisizione delle segnalazioni in piattaforma applicativa. Per la segnalazione con incontro diretto la dovuta informativa è fornita dal Responsabile della Prevenzione della Corruzione e della Trasparenza della **Provincia di Ancona**.
Accesso (art. 15) e Portabilità dei dati (art. 20)	Diritto di accesso garantito al soggetto segnalante tramite codice rilasciato post invio della segnalazione. Tenendo sempre in debito conto la tutela del soggetto segnalante, l'eventuale esercizio di altri diritti previsti dall'ordinamento europeo e nazionale (segnatamente l'accesso ai documenti amministrativi, l'accesso civico e l'accesso ai dati personali, cfr. art. 12, comma 8, del Decreto D.lgs. 24/2023, in riferimento agli artt. 22 e ss. della l. n. 241/1990 e all'art. 5 e ss. del d.lgs. 33/2013, nonché art. 13, comma 3, del Decreto, in riferimento agli artt. 15-22 del Regolamento e all'art. 2-undecies del Codice) è sottoposto a deroghe e limitazioni all'esercizio da parte del soggetto segnalato. Il diritto alla Portabilità dei dati non risulta applicabile.
Rettifica (art. 16) e Diritto all'oblio (art.	Il segnalante può effettuare integrazioni e modifiche. Ai sensi dell'art. 22 del D.lgs. 24/2023, le rinunce e le transazioni, integrali o parziali, che hanno per oggetto i diritti e le tutele previsti dal decreto non sono

[1] I diritti previsti agli artt. 15-22 GDPR non possono essere esercitati né con richiesta al titolare del trattamento né con reclamo al Garante per la Protezione dei dati Personali, qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte.

17) e Obbligo di notifica (art. 19)	valide, salvo che siano effettuate nelle forme e nei modi di cui all'articolo 2113, quarto comma, del Codice civile. L'Obbligo di notifica non risulta applicabile. I diritti di rettifica, oblio e notifica non si applicano al soggetto segnalato.
Limitazione e opposizione trattamento (art. 18, 19 e 21) e reclami (artt. 41, 43, 57)	I diritti di limitazione e opposizione non si applicano al soggetto segnalato. In ogni caso è possibile proporre reclamo all'Autorità Garante sia da parte dei soggetti segnalanti che segnalati.
Rapporti con i Responsabili del trattamento (art. 28)	Nomina dei soggetti delegati nella veste di responsabile del trattamento di dati personali con istruzioni specifiche, con particolare riguardo alla necessità di conservazione in massima sicurezza. Audit periodici della piattaforma.
Garanzie riguardanti trattamenti internazionali (capo V)	Non sono previste esportazioni di dati fuori dalla UE (datacenter posizionato in Italia).
Consultazione preventiva (articolo 36)	Consultazione preventiva non effettuata in quanto il trattamento anche in ragione delle misure adottate dal titolare non presenta rischi elevati per i diritti e le libertà dell'interessato.
Gestione rischi per i diritti e le libertà degli interessati	
Impatto potenziale per i diritti e le libertà degli interessati	**ALTO**
Valutazione della probabilità	**MEDIO BASSA**
Livello di rischio rilevato	RISCHIO = IMPATTO (**ALTO**) X PROBABILITÀ (**MEDIO BASSA**) = **MEDIO**
Fonti di rischio (Accesso illegittimo, modifica indesiderata, scomparsa dei dati)	Valore dato dalla Riservatezza: **MEDIO** Valore dato dalla Integrità: **MEDIO** Valore dato dalla Disponibilità: **MEDIO** Valore dato dalla Resilienza: **MEDIO** Valore dato dalla Accountability: **MEDIO**
Risultanze complessive dell'Analisi del rischio	Livello di rischio complessivo: **MEDIO** (vedi Allegato 1 – Report analisi dei rischi piattaforma Whistleblowing)
Misure previste per gestire i rischi (art. 35, paragrafo 7, lettera d)	Vedi misure attive indicate nel documento analisi dei rischi. Attivi soltanto protocolli TLS 1.2 e 1.3 Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema è protetta con chiave asimmetrica personale e protocollo a curve ellittiche (*Cipher Negotiated* di tipo "TLS_AES_256_GCM_SHA384, 384 bit ECDH (P-384)") per ciascun utente avente accesso al sistema e ai dati delle segnalazioni. Nessun dato è salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento.

	L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password. L'applicativo implementa un sistema di audit log sicuro e *privacy preserving* atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing. I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent. Altri elementi di sicurezza implementati: • sistema progettato in conformità alla norma ISO 27001:2022; • crittografia completa dei dati delle segnalazioni degli informatori e delle comunicazioni dei destinatari; • supporto dell'anonimato digitale con l'integrazione di Tor; • supporto HTTPS integrato con lo standard TLS 1.3 (classificazione SSLabs A+); • registrazione automatica gratuita del certificato digitale (Let's Encrypt); • non sono state rilevate vulnerabilità tecniche di particolare gravità, comunque facilmente risolvibili; • test di penetrazione multipli con rapporti pubblici completi; • conformità agli standard di settore e alle best practice per la sicurezza delle applicazioni (OWASP); • il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238; • *sandboxing* di rete integrato con iptables; • *sandboxing* dell'applicazione integrato con AppArmor; • protezione completa contro gli invii automatici (prevenzione dello spam); • soggetto a continue revisioni tra pari e controlli di sicurezza periodici; • supporto PGP per notifiche e-mail crittografate e download di file crittografati; • non lascia tracce nella cache del browser. L'appuntamento presso l'ufficio del Responsabile della Prevenzione della Corruzione e della Trasparenza della **Provincia di Ancona** non è tracciato, né rispetto al momento, né rispetto al soggetto segnalante, ferme restando le successive necessarie attività di riconoscimento e verbalizzazione.
Implementazione (rapida) di un sottoinsieme di ulteriori/successive misure di sicurezza	
Elenco sistemi utilizzati nel trattamento	Sistema di virtualizzazione; Virtual machine isolata e dedicata alla sola piattaforma; Whistleblowing; Piattaforma per la gestione informatizzata della segnalazione.
Misure di sicurezza da adottare per attenuare il rischio	Migliorare le indicazioni ai soggetti segnalanti al fine di evitare di lasciare traccia in più dispositivi o sistemi: ad esempio utilizzare sistemi al di fuori della rete dell'Organizzazione, con navigazione anonima.
Misure di sicurezza consigliate per attenuale il rischio	Eliminare la vulnerabilità di livello medio riscontrata (CVSS: 5.9 - NVT: SSL/TLS: BREACH attack against HTTP compression).

Ulteriori misure di sicurezza per innalzare la maturità del sistema	Effettuare periodici Vulnerability assessment della piattaforma. Simulare segnalazioni al fine di verificarne la correttezza del processo.
Altre Info utili alla valutazione	N/A
Risultanze ricalcolo Analisi del rischio	Livello di rischio complessivo: Accettabile con riserva di adozione delle misure indicate.
Parere del DPO	Si rilascia parere positivo considerato l'obbligo di legge e la piattaforma utilizzata.
Indicazioni del DPO (art. 35, par. 2)	Accettate.
Opinioni interessati o loro rappresentanti (art. 35, par. 9)	Considerata la tipologia di servizio non si è ritenuto necessario richiedere parere agli interessati. Resta fermo l'ascolto di ogni istanza da parte dei loro rappresentanti.
Esito finale della valutazione	In funzione dell'analisi effettua il trattamento in oggetto ha un livello di rischio accettabile che non necessita di comunicazione all'Autorità Garante secondo quanto previsto dall'art. 36 GDPR "Consultazione preventiva". Si consiglia comunque di adottare dei controlli in itinere, con audit specifici, in modo da verificare che le attività di trattamento siano effettuate secondo indicazioni; è necessario registrare evidenze dell'audit e relative prescrizioni in caso di non conformità rilevate.
Note	Nessuna
Versioning DPIA	Versione 02 del 04/08/2023 redatta da: DPO e team.