Valutazione di impatto sui trattamenti di dati personali effettuati a mezzo di “Whistleblowing”, per la segnalazione di violazioni del diritto dell'Unione europea ai sensi del nuovo d.lgs. 24/2023

Sommario

1 PREMESSA

La presente Valutazione di impatto sulla protezione dei dati personali (DPIA) è redatta ai sensi dell'art. 35 Regolamento (UE) 2016/679, da Fondazione Mondinsieme del comune di Reggio Emilia di seguito anche "Fondazione" o "Organizzazione"), in qualità di Titolare del trattamento, per valutare l'impatto sui diritti e le libertà degli interessati e la conformità alla normativa in materia di protezione dei dati personali, dei trattamenti di dati personali effettuati per la procedura di Whistleblowing, ai sensi del d.lgs. 24/2023

Il Regolamento Europeo 2016/679 (di seguito "GDPR"), divenuto applicabile a partire dal 25 maggio 2018, impone al titolare del trattamento la responsabilità di adottare tutte le misure necessarie al fine di garantire la sicurezza e la protezione dei dati.

L'art. 35 del GDPR prescrive l'obbligo, a carico del Titolare, prima di procedere al trattamento, di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati "*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. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*". La conduzione di una valutazione d'impatto preventiva rispetto al trattamento risulta attività coerente con i principi di protezione dei dati fin dalla progettazione per impostazione predefinita (art. 25 GDPR e considerando 78) (di seguito anche "DPIA", data processing impact assessment).
Inoltre, l'art. 13 D.lgs. 24/2023 prevede esplicitamente di condurre una valutazione di impatto sul trattamento inerente la segnalazione di condotte illecite.
Al fine di garantire il rispetto degli obblighi di riservatezza e protezione dei dati personali di cui agli artt. 12-13 D.Lgs. 24/2023, il Titolare del trattamento analizza con la presente valutazione le misure di sicurezza predisposte con la "PROCEDURA PER LA GESTIONE DELLE SEGNALAZIONI INTERNE di violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'amministrazione di cui il segnalante è venuto a conoscenza nel contesto lavorativo (WHISTLEBLOWING).
La procedura ha predisposto i canali di segnalazione interni e le tutele per i segnalanti e i segnalati.

Tra i canali di segnalazioni interni, oltre al canale orale, è prevista la piattaforma informatica di segnalazione interna basata su software libero ed open-source denominato "WhistleblowingPA", Servizio di whistleblowing software as a service (SaaS), basato su GlobaLeaks Free and Open Source Software (di seguito denominato Sistema), realizzato da Whistleblowing Solutions Impresa Sociale in collaborazione con Trasparency International Italia, per la segnalazione di violazioni del diritto dell'Unione ai sensi del d.lgs. 24/2023.

Il documento di Valutazione di Impatto elenca, dunque, i trattamenti previsti, affrontandone la natura, l'ambito di applicazione, il contesto e le finalità, allo scopo di valutarne la necessità e la proporzionalità, nonché di gestire i potenziali rischi per i diritti e le libertà delle persone fisiche da essi derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo.

La realizzazione di una DPIA costituisce un processo continuativo, pertanto la valutazione dei rischi e le misure poste in essere per contrastarli devono essere soggette a continuo monitoraggio e revisione. Sebbene l'art. 35, par. 11 GDPR preveda che la valutazione d'impatto debba essere riesaminata ogni qualvolta insorgano variazioni del rischio rappresentato dalle attività relative al trattamento, il Titolare si impegna a rinnovare la presente valutazione affinché sia aggiornata in relazione a possibili evoluzioni del progetto, anche nel rispetto delle buone prassi di cui alle Linee Guida n. 248 del WP 29, secondo le *quali "una valutazione d'impatto va riesaminata continuamente e va rivalutata con regolarità"*.

2 CONTESTO

L'art. 35, par. 7, GDPR prevede che la DPIA contenga almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito 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.

Spetta al Titolare del trattamento garantire lo svolgimento della DPIA (art. 35, par. 2, GDPR). La conduzione materiale della DPIA può essere affidata a un altro soggetto, interno o esterno all'organismo; tuttavia, la responsabilità ultima dell'adempimento ricade sul Titolare.
La presente valutazione d'impatto è condotta dall'organizzazione, in qualità di Titolare del trattamento.

2.1 Quale è il trattamento in considerazione?

I dati personali sono trattati per le finalità relative agli adempimenti e attività connesse alla raccolta e gestione delle segnalazioni di violazioni commesse ai danni dell'interesse pubblico (cd. Whistleblowing), rivolte agli organi legittimati ad intervenire.
La base giuridica prevede l'esecuzione di un compito di interesse pubblico nel rispetto degli obblighi previsti dalle leggi e dai regolamenti vigenti in materia.

Il soggetto, che intende effettuare una segnalazione, può utilizzare il Sistema per trasmettere testi e file a supporto della segnalazione stessa, rivolti al RESPONSABILE DELLA GESTIONE DELLE ISTANZE del Titolare.
All'arrivo di una segnalazione, il RESPONSABILE DELLA GESTIONE DELLE ISTANZE la prende in carico attraverso il canale di segnalazione predisposto. Il RESPONSABILE DELLA GESTIONE DELLE ISTANZE opera all'interno del Sistema attraverso opportuni step di avanzamento/annullamento del procedimento che possono essere visualizzati dal segnalante, utilizzando le credenziali di sistema.

2.2 Quali sono le responsabilità connesse al trattamento?

Il Titolare del trattamento dei dati è la Fondazione, che ha in utilizzo il servizio della piattaforma-applicativa. La gestione del canale di segnalazione interno informatico è effettuato da Whistleblowing Solutions IS Srl, che deve essere nominato ai sensi dell'art.28 del GDPR quale Responsabile del trattamento dei dati personali.

2.3 Ci sono standard applicabili al trattamento?

La normativa e gli standard di riferimento del presente documento sono:

- Articolo 6 del GDPR;
- Articolo 35 del GDPR;
- Considerando n. 71, 84, 89, 90, 91, 92, 93 e 95 del GDPR;
- Linee Guida n. 248 del WP 29, concernenti "la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilite se un trattamento possa presentare un rischio elevato" ai sensi del GDPR, la cui ultima versione è datata 4 ottobre 2017;

Il trattamento dei dati viene inoltre svolto in conformità agli standard, ovvero:

- IEC/ISO 27001 - IEC/ISO 27017/ ISO27018;
- Certificazione CSA STAR Self-Assessment;
- D.Lgs. 24/2023

- Nuove linee guida Anac rilasciate ai sensi dell'art. 10 D.Lgs,. 24/2023 (testo in consultazione)

Inoltre, Whistleblowing Solutions IS Srl risulta qualificata al marketplace AgID (oggi da ACN – Agenzia per la cybersecurity nazionale) per il cloud della PA relativamente alla categoria "Servizi per l'information technology, IT Security, Content Management".

3 DATI, PROCESSI E RISORSE DI SUPPORTO

3.1 Quali sono i dati trattati?

Con riferimento al canale di segnalazione informatico interno, i dati sono raccolti tramite il modulo elettronico di segnalazione attraverso il servizio web online, il modulo è costituito da due parti distinte:

- la prima è relativa all'identità del segnalante:

o Nome
o Cognome
o Codice fiscale
o E-mail
o Telefono

- la seconda è relativa al contenuto della segnalazione:

In questa seconda parte, la segnalazione potrebbe contenere vari dati personali non predeterminabili a monte, in quanto la segnalazione è di tipo descrittivo.

Con riferimento al canale di segnalazione interna orale, i contenuti della segnalazione non sono predeterminabili dall'organizzazione. Il segnalante può telefonare da numero anonimo o in chiaro e indicare la propria identità e un punto di contatto per ricevere aggiornamenti o trascrizioni dei messaggi vocali inviati.

3.2 Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Come specificato nella PROCEDURA PER LA GESTIONE DELLE SEGNALAZIONI INTERNE, il segnalante invia la segnalazione al RESPONSABILE DELLA GESTIONE DELLE ISTANZE tramite uno dei canali istituiti dalla Fondazione: canale scritto o orale.
Il canale interno di segnalazione scritta si sviluppa per mezzo del sistema informatico.
Il canale interno di segnalazione orale, si concretizza tramite sistema di messaggistica vocale o tramite incontro dedicato.

Il Sistema informatico consente di segnalare i fatti e le condotte illecite, tutelando la riservatezza del segnalante, attraverso la compilazione di un "form" distinto in due parti: dati personali e contenuto della segnalazione.

Successivamente all'inoltro della segnalazione, il segnalante riceve dal sistema un Codice identificativo univoco.

Il RESPONSABILE DELLA GESTIONE DELLE ISTANZE riceve una e-mail sulla casella di posta elettronica istituzionale dedicata alla ricezione delle segnalazioni che notifica la presenza di una nuova segnalazione nel portale del Whistleblowing, a cui accede dal link presente nel corpo dell'e-mail.
Il RESPONSABILE DELLA GESTIONE DELLE ISTANZE è l'unico soggetto ad avere le credenziali di accesso alla casella di posta elettronica istituzionale dedicata alla ricezione delle segnalazioni e al portale online.
Il portale richiede username e password in possesso del solo RESPONSABILE DELLA GESTIONE DELLE ISTANZE per accedere alla lista delle Segnalazioni. La password dovrà essere cambiata, a cura del RESPONSABILE DELLA

GESTIONE DELLE ISTANZE ogni 90 giorni.
Il RESPONSABILE DELLA GESTIONE DELLE ISTANZE per visualizzare la nuova segnalazione dovrà selezionarla dalla lista.
Il portale consente una registrazione cronologica delle segnalazioni con registrazione della data e dell'ora di ricezione delle segnalazioni.
Il RESPONSABILE DELLA GESTIONE DELLE ISTANZE potrà autorizzare un soggetto istruttore a coadiuvarlo nella gestione dell'istanza.
Il soggetto istruttore è soggetto ai medesimi obblighi di riservatezza del RESPONSABILE DELLA GESTIONE DELLE ISTANZE la cui violazione è punita a livello disciplinare.
In ogni caso, il RESPONSABILE DELLA GESTIONE DELLE ISTANZE avrà l'onere di mantenere riservati i dati identificativi del segnalante e il contenuto della segnalazione.

Per le segnalazioni tramite il canale orale è istituito un sistema di registrazione di messaggistica vocale.

Viene fornito dall'organizzazione al RESPONSABILE DELLA GESTIONE DELLE ISTANZE un telefono cellulare e una sim telefonica dedicata alla ricezione delle segnalazioni orali.
Sull'utenza telefonica viene attivata a cura dell'organizzazione la segreteria telefonica con registrazione di messaggio con presentazione vocale dell'informativa del trattamento dei dati personali e delle informazioni necessarie per reperire il testo completo di tale informativa.
La segreteria così attivata consente l'acquisizione delle segnalazioni orali.
Ricevuta una segnalazione orale il RESPONSABILE DELLA GESTIONE DELLE ISTANZE provvederà a trascrivere il contenuto della segnalazione ricevuta nel registro delle segnalazioni orali.
Prima della registrazione viene chiesto il consenso del segnalante e un punto di contatto se il segnalante volesse ricevere la trascrizione da verificare, rettificare, confermare nei casi di legge.
Il contenuto della segnalazione e il nominativo del soggetto segnalante saranno inseriti in una busta chiusa al cui esterno verrà indicato solo il numero progressivo di segnalazione.
Il registro delle segnalazioni, la segnalazione, il nominativo del segnalante nonché tutti gli accertamenti istruttori del caso saranno conservati presso la sede dell'organizzazione in armadio dedicato provvisto di chiusura le cui chiavi sono nella esclusiva disponibilità del RESPONSABILE DELLA GESTIONE DELLE ISTANZE .
Il RESPONSABILE DELLA GESTIONE DELLE ISTANZE potrà autorizzare un soggetto istruttore a coadiuvarlo nella gestione dell'istanza.
Il soggetto istruttore è soggetto ai medesimi obblighi di riservatezza del RESPONSABILE DELLA GESTIONE DELLE ISTANZE la cui violazione è punita a livello disciplinare. In ogni caso, il RESPONSABILE DELLA GESTIONE DELLE ISTANZE avrà l'onere di mantenere riservati i dati identificativi del segnalante e il contenuto della segnalazione.
Solo se richiesto dal segnalante, il RESPONSABILE DELLA GESTIONE DELLE ISTANZE potrà fissare incontri diretti entro un termine ragionevole in luogo di volta in volta stabilito, previa presentazione dell'informativa del trattamento dei dati personali e delle informazioni necessarie per reperire il testo completo di tale informativa.
Dell'incontro viene redatto apposito verbale che verrà conservato con le modalità previste per la conservazione delle segnalazioni scritte. In caso di verbale, la persona segnalante può verificare, rettificare, confermare il verbale dell'incontro mediante sottoscrizione del verbale.

3.3 Quali sono le risorse di supporto ai dati?

- Software "WhistleBlowing PA
- Gestore telefonico

3.4 Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento è effettuato in adempimento agli specifici obblighi di legge che gravano sul Titolare (Legge 190/2012; Direttiva EU 2019/1937; D. Lgs 24/2023). Le finalità sono rese note agli interessati mediante specifica informativa sul trattamento.
Il trattamento si svolge nel rispetto dei principi normati dall'art. 5 del GDPR e dei diritti dell'interessato disciplinati nel Capo III dello stesso. Il trattamento è effettuato con modalità - automatizzate e non - e comprende le operazioni o il complesso di operazioni necessarie per il perseguimento delle finalità di cui al precedente punto 2, senza profilazione dei dati.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati).

3.5 Quali sono le basi legali che rendono lecito il trattamento?

I dati richiesti sono necessari per il rispetto della normativa, in particolare del nuovo d. lgs. 24/2023, in virtù del quale sono disciplinate nel nostro ordinamento giuridico misure finalizzate a favorire l'emersione delle fattispecie di violazione, nota nei paesi anglosassoni col termine di "whistleblowing" (art. 6 par. 1 lett. C GDPR)

Nel caso di attivazione del procedimento disciplinare da parte dell'Amministrazione contro il presunto autore della condotta segnalata, ai sensi dell'art.12 co. 5 D.Lgs. 24/2023, qualora l'identità del segnalante sia indispensabile per la difesa del soggetto cui è stato contestato l'addebito disciplinare, viene richiesto il consenso del segnalante, ex art. 6, par. 1, lett. a) del GDPR, per poterne rilevare l'identità.

Con riferimento ai dati di particolari categorie che possono potenzialmente emergere nell'ambito delle segnalazioni, sebbene in modo residuale e non predeterminabile dall'Ente, gli stessi saranno trattati esclusivamente ai sensi dell'art. 9 GDPR e art. 2 sexies D.Lgs. 196/2003, ovvero qualora il trattamento sia necessario per motivi di interesse pubblico rilevante (es. Attività di controllo o ispettive; accertamento di responsabilità civile, disciplinare, contabile del personale dipendente) o qualora il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria.

Con riferimento ai dati personali relativi a condanne penali o reati che possano eventualmente emergere dal contenuto della segnalazione, gli stessi sono trattati esclusivamente ai sensi dell'art. 10 GDPR.

3.6 I dati sono esatti e aggiornati?

L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata.
Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.

3.7 Qual è il periodo di conservazione dei dati?

Il periodo di conservazione delle segnalazioni e della relativa documentazione è limitato, ai sensi dell'art. 5 del GDPR, nonché dell'art. 14 d. lgs. 24/2023, al 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.
Il RESPONSABILE DELLA GESTIONE DELLE ISTANZE , in ogni caso, una volta aperta l'istruttoria, valuta se la segnalazione sia rilevante. In caso di irrilevanza o improcedibilità, i dati verranno cancellati.
Successivamente alla decorrenza del termine dei cinque anni, qualora rimangano necessità di conservazione per la tutela giurisdizionale o stragiudiziale della Fondazione, i dati verranno conservati per garantire tale finalità.
Le segnalazioni vengono conservate dal canale informatico per un periodo di 18 mesi dalla ricezione. Il fornitore del canale di segnalazione interno, nel "ACCORDO IN MERITO AL TRATTAMENTO DI DATI PERSONALI Ai sensi dell'art. 28 del Regolamento UE 2016/679" si impegna a cancellare i dati entro 15 giorni dalla richiesta di disattivazione del servizio.

4 PRINCIPI FONDAMENTALI

Le Modalità di gestione delle segnalazioni sono effettuate in accordo al d. lgs. 24/2023 in materia di tutela degli autori di segnalazioni di violazioni del diritto dell'Unione.

4.1 Misure a tutela dei diritti degli interessati

4.1.1 Come sono informati del trattamento gli interessati?

Nel servizio online di inserimento della segnalazione, il segnalante è tenuto a prendere visione dell'informativa privacy prima di procedere all'invio dei dati.

In caso di canale di segnalazione orale, viene fornita l'informativa breve per indicare dove reperire l'informativa estesa. Il Titolare pubblica sul proprio sito web istituzionale l'informativa estesa sul trattamento dei dati ai sensi dell'art. 13-14 GDPR per consentire non solo ai segnalanti, ma anche ai potenziali segnalati, di poter verificare le finalità e modalità di trattamento dei loro dati personali.

4.1.2 Ove applicabile: come si ottiene il consenso degli interessati?

Il trattamento in oggetto non si fonda sul consenso degli interessati, bensì sull'adempimento degli obblighi di legge di cui alle disposizioni richiamate nel par. 3.4.
È comunque presente all'interno del Sistema una maschera per l'espressione del consenso del segnalante, per la rilevazione della sua identità in caso di procedimento disciplinare.

4.1.3 Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

L'art. 2-undecies, comma 1, lett. f) del D.Lgs. 196/2003 esclude l'esercizio dei diritti di cui agli art. 15-22 qualora gli stessi possano determinare la perdita di riservatezza dell'identità del segnalante.

Il segnalante, in qualità di interessato, può esercitare i diritti previsti dal Capo III del GDPR ed in particolare il diritto di accedere ai propri dati personali. A tal fine l'interessato/a potrà rivolgersi al Titolare del trattamento.

4.1.4 Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

L'art. 2-undecies, comma 1, lett. f) del D.Lgs. 196/2003 esclude l'esercizio dei diritti di cui agli art. 15-22 qualora gli stessi possano determinare la perdita di riservatezza dell'identità del segnalante.

Il richiedente, in qualità di interessato, può esercitare i diritti previsti dal Capo III del GDPR ed in particolare il diritto di chiedere la rettifica dei dati o la cancellazione fatta salva l'esistenza di motivi legittimi da parte del Titolare. A tal fine l'interessato/a potrà rivolgersi al Titolare del trattamento.

4.1.5 Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

L'art. 2-undecies, comma 1, lett. f), D.lgs. 196/2003 esclude l'esercizio dei diritti di cui agli art. 15-22 qualora gli stessi possano determinare la perdita di riservatezza dell'identità del segnalante.

Il richiedente, in qualità di interessato, può esercitare i diritti previsti dal Capo III del GDPR ed in particolare il diritto di chiedere la limitazione, nonché di opporsi al loro trattamento fatta salva l'esistenza di motivi legittimi da parte del Titolare. A tal fine l'interessato/a potrà rivolgersi al Titolare del trattamento.

4.1.6 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

L'organizzazione, in qualità di Titolare, deve nominare Whistleblowing Solutions IS Srl, quale Responsabile, attraverso opportuno atto formale, così come previsto dall'art. 28 del GDPR, in cui vengono esplicitati gli obblighi che il responsabile assume nei confronti del Titolare.

4.1.7 In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Non è previsto alcun trasferimento di dati all'estero da parte del Responsabile del trattamento.

4.2 Misure esistenti o pianificate – Analisi dei rischi e valutazione DPIA

Considerate le misure tecniche e organizzative predisposte dal Titolare del trattamento con la Procedura per la gestione delle segnalazioni interne, si intende verificare se il rischio residuo sia accettabile per garantire le tutele assicurate dagli art.12-13e ss. D.Lgs. 24/2023.
Oltre alle misure organizzative predisposte dalla Fondazione con la procedura e le politiche interne, è necessario considerare le misure tecniche offerte dai soggetti esterni ai quali la Fondazione di affida per garantire un livello adeguato di protezione dei dati personali.
Infatti, la dimensione e l'ambito di operatività della Fondazione non gli consentono di predisporre direttamente i

canali di segnalazione interna secondo gli standard di sicurezza allo stato dell'arte. Per tale motivo, il Titolare del trattamento ha inteso affidare la gestione tecnica dele segnalazioni a un soggetto esterno, vincolando lo stesso con apposite clausole contrattuali ai sensi dell'art. 28 e 32 GDPR.

I principali termini utilizzati nell'ambito della DPIA sono:

Probabilità [**P**]: valutazione della frequenza di accadimento di una minaccia, in funzione delle vulnerabilità in essere e di eventuali contromisure implementate;

Impatto [**I**]: indicazione della gravità di un incidente che comprometta la riservatezza, l'integrità e la disponibilità di processi, dati, informazioni incluse nel perimetro di applicazione della normativa

Minaccia [**M**]: evento potenziale, accidentale o deliberato, che, nel caso accadesse, produrrebbe un danno per l'interessato;

Vulnerabilità [**V**]: debolezza intrinseca del sistema informativo o del sistema informatico che, qualora si realizzasse una minaccia che la sfrutti, produrrebbe un danno all'interessato;

Rischio Privacy [**RP**]: combinazione di impatto per l'interessato e della probabilità di accadimento di una minaccia che possa compromettere la riservatezza, l'integrità o la disponibilità di un dato personale ad esso riferito;

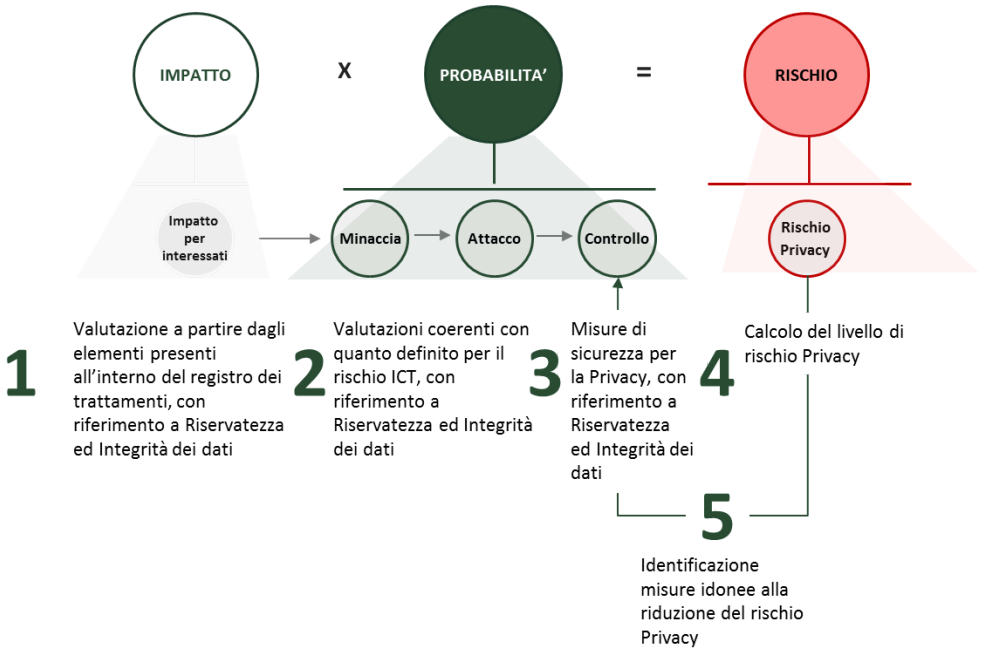
Contromisure [**C**]: soluzioni organizzative, procedurali o tecnologiche che possono essere implementate al fine di mitigare il Rischio Privacy associato ad ogni sistema o archivio e quindi diminuire il Rischio;

Soglie di accettazione del rischio [**S**]: definizione del livello massimo di rischio accettato superato il quale si rende necessaria l'implementazione delle contromisure.

La metodologia di valutazione dei rischi si articola in 5 fasi, descritte nell'immagine di seguito riportata.

Le fattispecie oggetto di analisi rispecchiano le categorie di informazioni previste dal Registro dei trattamenti di cui all'art. 30 del GDPR.

La tabella di seguito riportata contiene una sintesi delle informazioni che descrivono il trattamento e ne permettono l'identificazione.



Al fine di valutare gli **impatti sui diritti e le libertà dei soggetti interessati dal trattamento**, si considera che la perdita della riservatezza potrebbe comportare stress per i segnalanti e, nei casi più gravi, a discriminazioni e ritorsioni sul luogo di lavoro.
La perdita di integrità e disponibilità dei dati potrebbe limitare il diritto di difesa del soggetto segnalato.
Tali impatti, considerati a partire dal rischio inerente, devono comunque essere considerati già ridotti dalle tutele predisposte per legge dal D.Lgs. 24/2023 che prevedono il divieto di ritorsione tramite licenziamenti, sospensioni, retrocessioni, misure disciplinari, discriminazioni e altri comportamenti espressamente richiamati.
Pertanto, dal momento che il rischio inerente è in parte mitigato dalla previsione di tutele ex lege, cui la Fondazione è tenuto, il rischio inerente che la Fondazione deve essere in grado di evitare con la predisposizione di misure di sicurezza per la protezione dei dati personali riguarda lo stress che l'interessato dovrebbe patire per attivare le tutele e le misure di sostegno in caso di un danno ingiusto determinato (ancorché non direttamente causato) dalla perdita di riservatezza dei dati personali.
Con riferimento alla perdita dell'integrità e disponibilità dei dati, il D.Lgs. 24/2023 individua misure a tutela del diritto di difesa del soggetto segnalato. Pertanto, l'Ente dovrà garantire la corretta applicazione della procedura e degli obblighi di legge
Alla luce di quanto sopra esposto, si ritiene che le **minacce** rilevanti per il rischio privacy siano, dunque le seguenti:

- Attacchi informatici
- Abuso di privilegi di accesso
- Modifica non autorizzata dei dati
- Errori nei processi di elaborazione dei dati
- Inefficiente gestione del dato
- Perdita integrità per guasto HW
- Interrogazioni improprie su basi dati
- Furto o smarrimento di apparati hardware
- Intercettazione delle comunicazioni
- Utilizzo improprio di software o servizi
- Perdita disponibilità per guasto HW
- Cancellazione volontaria o accidentale dei dati
- Dipendente infedele
- Mancanza di formazione del personale preposto

La **verosomiglianza** del rischio deve essere considerata anche alla luce del contesto e della dimensione del Titolare del trattamento, sia in ordine al numero di dipendenti o collaboratori che di potenziali segnalanti, in entrambi i casi limitati. Inoltre, deve essere considerata l'efficacia delle misure finora applicate, per le quali si monitorerà il numero di segnalazioni e le eventuali violazioni riscontrate.
Per la **riduzione del rischio inerente individuato**, è necessario distinguere le misure organizzative direttamente in capo al Titolare del trattamento, rispetto alle misure tecniche che devono essere applicate dal responsabile del trattamento che mette a disposizione il proprio know how nella gestione di canali di segnalazione interni.
Whistleblowing Solutions Impresa Sociale ha implementato le seguenti misure tecniche (Allegato_1 Documentazione a supporto del titolare per la valutazione di impatto sulla protezione dei dati):

CRITTOGRAFIA
L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington. Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+. Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni. Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento Il sistema è installato su sistema operativo Linux su

cui è attiva Full Disk Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto.
La descrizione delle misure di sicurezza applicate per la conservazione delle chiavi crittografiche è documentata in "MODALITÀ DI CONSERVAZIONE DELLE CHIAVI CRITTOGRAFICHE" di Whistleblowing PA. La Fondazione può richiedere a Whistleblowing PA di ricevere le chiavi crittografiche.

CONTROLLO DEGLI ACCESSI LOGICI
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. Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238. Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

TRACCIABILITÀ
L'applicativo GlobaLeaks 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. I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.

ARCHIVIAZIONE
L'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM. 10/12 Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.

GESTIONE DELLE VULNERABILITÀ TECNICHE
L'applicativo GlobaLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review. A questi si aggiunge la peer review indipendente realizzata dalla crescente comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente.

BACKUP
I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.

MANUTENZIONE
È prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza. Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti. Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti

SICUREZZA DEI CANALI INFORMATICI
Tutte le connessioni sono protette tramite protocollo TLS 1.2+ Le connessioni amministrative privilegiate sono mediate tramite accesso VPN e connessioni con protocollo SSH.

SICUREZZA DELL'HARDWARE
I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e

barriere fisiche presidiate 7x24. I datacenter del fornitore IaaS sono certificati ISO27001.

GESTIRE GLI INCIDENTI DI SICUREZZA E LE VIOLAZIONI DEI DATI PERSONALI

Whistleblowing Solutions ha definito una procedura per la gestione delle violazioni dei dati personali.

LOTTA CONTRO IL MALWARE

Tutti i computer del personale di Whistleblowing e dei sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale ed il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware. Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.

Il Titolare del trattamento ha individuato le misure essenziali del trattamento determinando finalità e durata del trattamento, mentre il Responsabile del trattamento ha individuato le c.d. misure non essenziali con propria autonoma iniziativa, sulla base del proprio know how tecnico. Nel contratto di nomina il Responsabile del trattamento è vincolato a garantire le misure di sicurezza in autonomia in quanto "*il Fornitore dichiara e garantisce (i) di mantenere, ogni e qualsiasi misura di sicurezza idonea a prevenire i rischi di distruzione, perdita, anche accidentale, dei Dati Personali nonché di accesso non autorizzato o trattamento illecito dei medesimi come previsto nel Contratto di servizi e (ii) che tali misure sono conformi anche alle misure di sicurezza necessarie e conformi ai principi di cui all'art. 32 del Regolamento Privacy, nonché ogni altra misura obbligatoria di legge. Con riferimento al trattamento di Dati Personali svolti con l'ausilio di strumenti elettronici per la prestazione dei Servizi e la gestione del database per conto del Committente, il Responsabile si impegna ad attuare le seguenti misure: i. scegliere gli amministratori di sistema tra quei soggetti dotati di esperienza, capacità ed affidabilità, in grado di garantire il pieno rispetto della normativa italiana in materia di protezione dei dati personali, ivi compreso il profilo relativo alla sicurezza; ii. nominare gli amministratori di sistema individualmente, elencando analiticamente gli ambiti di operatività consentiti a ciascun amministratore di sistema in relazione al proprio profilo di autenticazione; iii. tenere un elenco aggiornato dei soggetti nominati amministratori di sistema e, su richiesta, mettere tale elenco a disposizione del Committente e/o delle autorità competenti;Il Fornitore si impegna a verificare regolarmente l'idoneità delle misure adottate*".

L'organizzazione del Titolare, a sua volta, ha adottato le seguenti misure organizzative come **piano d'azione per la mitigazione**:

- Nomina del RESPONSABILE DELLA GESTIONE DELLE ISTANZE , come da normativa di riferimento;
- Nomina del sostituto del RESPONSABILE DELLA GESTIONE DELLE ISTANZE , nei casi in cui si verifichi in capo a quest'ultimo una personale situazione di conflitto di interesse, un suo diretto coinvolgimento nel fatto segnalato, oppure una sua temporanea ed improvvisa assenza, nonché nomina del Collaboratore diretto del RESPONSABILE DELLA GESTIONE DELLE ISTANZE a supporto delle segnalazioni pervenute;
- Nomina del RESPONSABILE DELLA GESTIONE DELLE ISTANZE e del sostituto del RESPONSABILE DELLA GESTIONE DELLE ISTANZE a Designati del trattamento dei dati personali;
- Nomina del Collaboratore diretto del RESPONSABILE DELLA GESTIONE DELLE ISTANZE ad Autorizzato del trattamento dei dati personali;
- Approvazione della Procedura di gestione delle segnalazioni interne;
- Nomina di Whistleblowing Solutions IS SRL quale Responsabile del trattamento dei dati (inviare contratto di nomina sottoscritto, presente su https://www.whistleblowing.it/documentazione-tecnica/ a gdpr@whistleblowing.it)
- Pubblicazione dell'informativa al trattamento dei dati ai sensi dell'art. 13-14 GDPR sul sito web istituzionale;
- Registrazione di un messaggio di segreteria per indicare il sito web dove poter consultare il testo integrale dell'informativa privacy, con l'avviso che proseguendo si presta il consenso alla registrazione del messaggio e la richiesta di indicare un punto di contatto qualora si voglia ricevere il testo della trascrizione per verifica;
- Formazione del personale coinvolto;

- Nel caso in cui l'accesso al canale di segnalazione interno informatico è mediato da dispositivi firewall o proxy, il titolare del trattamento deve garantire la non tracciabilità del segnalante nel momento in cui viene stabilita la connessione anche mediante l'impiego di strumenti di anonimizzazione dei dati di navigazione (es. Accesso mediante rete TOR);

Per la riduzione del rischio si ritiene che le misure poste in essere siano accettabili per poter svolgere il trattamento. Le misure di sicurezza di cui si avvale la piattaforma WhistleblowingPa, unitamente alle misure organizzative adottate dall'organizzazione per gli altri canali di segnalazione e per la conduzione dell'istruttoria, sono ritenute in grado di mitigare tutte le minacce sopra esposte.

Si specifica inoltre che, con riferimento al canale di segnalazione orale, l'applicazione delle misure di sicurezza previste dalla normativa in materia di segnalazione delle violazioni del diritto dell'Unione è necessaria per la mitigazione dei rischi ai fini della tutela della riservatezza.
Pertanto, si valuta che riducano il rischio residuo in modo accettabile, in quanto comportano una diminuzione della verosimiglianza generale di accadimento.

L'introduzione ulteriore di misure di sicurezza sarebbe in contrasto con i principi del d. lgs 24/2023, con conseguente diminuzione eccessiva dell'operatività. Pertanto, dal momento che ai sensi dell'art. 32 GDPR le misure di sicurezza devono essere adottate anche *"tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento"*, si ritiene che la tutela del diritto in questione debba essere garantita in termini di efficienza accettabili sulla base delle misure introdotte.

5 CONCLUSIONI

In considerazione della natura, del contesto, delle tipologie di dati trattati e delle soluzioni tecnologiche descritte, il trattamento effettuato dal Servizio di raccolta e gestione delle segnalazioni di violazioni o irregolarità commesse ai danni dell'interesse pubblico (Whistleblowing), ai sensi del D.Lgs. 24/2023 e s.m.i., identifica un rischio accettabile dall'organizzazione in quanto si ritiene che le misure organizzative e tecniche siano idonee ad escludere i più gravi impatti di ritorsione e discriminazione, residuando minacce determinate da errore umano rilevante a livello disciplinare o accesso abusivo a sistema informatico determinato da dolo, penalmente perseguibile.

5.1 Allegati

- Informativa privacy, ex art. 13 GDPR, per gli interessati al trattamento;
- Accordo di nomina a responsabile del trattamento ex art.28 GDPR;
- Documento a supporto del titolare per la valutazione di impatto sulla protezione dei dati Whistleblowing pa;
- Procedura per la gestione delle segnalazioni interne di violazioni di disposizioni normative nazionali o dell'unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione di cui il segnalante è venuto a conoscenza nel contesto lavorativo (whistleblowing).

6 OPINIONE DEGLI INTERESSATI

La richiesta di opinione degli interessati, alla luce della quantità di potenziali segnalanti e segnalati legittimati ai fini della normativa, appare sproporzionata e impraticabile e pertanto non è dovuta come indicato dalla Linee guida sulla valutazione di impatto n. 248 del Working Party Article 29. L'invio di informativa alla rappresentanza sindacale, come previsto dalla normativa di legge applicabile, può considerarsi quale misura di compensazione, indicando che un estratto della Valutazione di impatto condotta è a disposizione degli stessi qualora richiesto.

Reggio Emilia, 26/05/2025
Gianluca Grasi
Il Titolare del Trattamento