Valutazione d'impatto (DPIA) del sistema di ricevimento e gestione delle segnalazioni interne WHISTLEBLOWING

Ai sensi dell'art. 35 REGOLAMENTO (UE) 2016/679

Titolare del trattamento	Comune di Toceno		
Responsabile della Protezione dei Dati personali (DPO/RPD):	Labor Service S.r.l. Dott.ssa Chiara Mittini		
Autori	• **Dott. Daniele Merola** Segretario Comunale nonchè RPCT • **Dott.ssa Chiara Mittini** Responsabile della Protezione dei Dati personali		
Data di emissione	31/01/2024	**Versione**	00

Sommario

1. Riferimenti normativi

La valutazione d'impatto (o, altrimenti detta, DPIA – *Data Protection Impact Assessment*) è una procedura prevista dall'articolo 35 del Regolamento (UE) 2016/679 (GDPR) che il titolare deve svolgere allorquando intraprenda un'attività di trattamento particolarmente delicata. Lo scopo è quello di verificare l'impatto del trattamento sui diritti e le libertà degli interessati, valutandone, da una parte, la necessità e la proporzionalità rispetto al fine da perseguire, dall'altra, l'idoneità delle misure di sicurezza approntate per annullare o almeno limitare i rischi di incidenti. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

Si riporta qui di seguito il testo integrale della citata norma, dove sono specificatamente indicate le condizioni al ricorrere delle quali è doverosa la valutazione d'impatto.

1. Quando un tipo di trattamento, allorché prevede in particolare l'**uso di nuove tecnologie**, **considerati la natura, l'oggetto, il contesto e le finalità** del trattamento, può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

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**.

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7. **La valutazione contiene** almeno:

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

b) una valutazione della **necessità e proporzionalità** dei trattamenti in relazione alle finalità;

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

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

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

11. 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.

2. Doverosità di svolgere la DPIA

I soggetti del settore pubblico sono tenuta a norma del D.Lgs. 24/2023 ad adottare un modello di ricevimento e gestione delle segnalazioni interne di whistleblowing che comporta il trattamento da parte dell'RPCT di informazioni su illeciti (dati giudiziari) commessi all'interno dell'ente rivelati da segnalanti la cui identità deve rimanere riservata e conoscibile solo dalle persone autorizzate.
Tali segnalazioni comportano un trattamento di dati personali che può rappresentare un rischio elevato per i diritti e le libertà delle persone fisiche, tenendo conto della natura, dell'oggetto, del contesto, delle finalità e delle eventuali nuove tecnologie utilizzate.
Pertanto, risulta obbligatoria la redazione del presente documento ai sensi dell'art. 35 GDPR anche alla luce dell'espressa previsione contenuta nell'art. 13, comma 6, del D.Lgs. 24/2023.

3. Contesto

3.1. Panoramica del trattamento

Quale è il trattamento in considerazione?
Il trattamento dei dati riguarda le persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica, di cui siano venute a conoscenza nel contesto lavorativo (c.d. Whistleblowing) ai sensi della L. 179/2017 e del D.lgs. 24/2023. Inoltre, il trattamento dei dati riguarda anche i soggetti a cui è attribuito l'illecito e gli eventuali altri soggetti coinvolti come i facilitatori, persone del medesimo contesto lavorativo legate al segnalante da uno

stabile legame affettivo o di parentela entro il quarto grado e i colleghi di lavoro del segnalante che hanno con detta persona un rapporto abituale e corrente.
Chi segnala fornisce informazioni che possono portare all'indagine, all'accertamento e al perseguimento dei casi di violazione delle norme, rafforzando in tal modo i principi di trasparenza e responsabilità delle istituzioni democratiche.
Garantire la protezione dei soggetti che si espongono con segnalazioni, denunce o con l'istituto della divulgazione pubblica, contribuisce all'emersione e alla prevenzione di rischi e situazioni pregiudizievoli per la stessa amministrazione e, di riflesso, per l'interesse pubblico collettivo.
Tale protezione è estesa anche a soggetti diversi da chi segnala, come il facilitatore o le persone menzionate nella segnalazione, a conferma dell'intenzione, del legislatore europeo e italiano, di creare condizioni per rendere l'istituto in questione un importante presidio per la legalità, per la concorrenza e per garantire il buon andamento e l'imparzialità delle pubbliche amministrazioni.
Il Comune, per adempiere a quanto richiesto dalla normativa, si avvarrà per l'istituzione del canale di segnalazione interno, di un soggetto esterno che fornisce la piattaforma di segnalazione e gestione degli illeciti. In particolare, tale soggetto, Whistleblowing Solutions Impresa Sociale S.r.l. (di seguito "Whistleblowing Solutions"), si occupa della gestione del sistema di whistleblowing per l'esecuzione di operazioni informatizzate di trattamento di dati personali relative alla raccolta e alla conservazione dei dati necessari per l'erogazione del servizio.
Il sistema di whistleblowing proposto da Whistleblowing Solutions avrà le seguenti caratteristiche:

ARCHITETTURA DI SISTEMA
L'architettura di sistema è principalmente composta da:
- Un cluster di due firewall perimetrali;
- Un cluster di due server fisici dedicati;
- Una Storage Area Network pienamente ridondata.

SOFTWARE IMPIEGATO
La piattaforma informatica di segnalazione è basata sul software libero ed open-source GlobaLeaks di cui Whistleblowing Solutions è co-autore e coordinatore di progetto.
In aggiunta a GlobaLeaks, utilizzato in via principale per l'implementazione del servizio, per finalità di pubblicazione, documentazione e supporto del progetto vengono utilizzate altre tecnologie a codice aperto e di pubblico dominio la cui qualità è indipendentemente verificabile.
Vengono anche in modo limitato utilizzate alcune note tecnologie proprietarie e licenziate necessarie per finalità di gestione infrastrutturale e backup professionale.
Vengono primariamente utilizzati le tecnologie open source:
- Debian/Linux (principale sistema operativo utilizzato);
- Postfix (mail server);
- Bind9 (dns server);
- OPNSense (firewall);
- OpenVPN (vpn).

Le limitate componenti software di natura proprietaria impiegate sono le seguenti:
- VMware, software di virtualizzazione;
- Veeam, software di backup;
- Plesk, software per realizzazione siti web di facciata del progetto.

Predisposizione dei sistemi virtualizzati:
- I server eseguono software VMware e vCenter abilitando funzionalità di High Availability;
- Su VMware vengono istanziate macchine virtuali Debian/Linux nelle sole version Long Term Support (LTS);
- Ogni macchina virtuale Debian implementa configurazione securizzata con: Full Disk Encryption (lvm/crypto), SecureBoot, Apparmor, Iptables;

- Entrambi i server fisici eseguono una macchina virtuale di Key Management 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 componenti il cluster.

ARCHITETTURA DI RETE
- L'architettura di rete prevede un firewall perimetrale e segregazione della rete in molteplici VLAN al fine di isolare le differenti componenti secondo loro differente natura al fine di limitare ogni esposizione in caso di vulnerabilità su una singola componente;
- Una VPN consente l'accesso alla gestione dell'infrastruttura a un limitato e definito insieme di amministratori di sistema;
- Ogni connessione di rete implementa TLS 1.2+;
- Ogni macchina virtuale istanziata vede esposizione di rete limitata all'effettiva necessità;
- Tutti i dispositivi utilizzati quali l'applicativo GlobaLeaks, Log di sistema e Firewall sono configurati per non registrare alcun tipo di log e/o informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP e User Agents;
- L'applicativo GlobaLeaks abilita la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

Quali sono le responsabilità connesse al trattamento?
Il Comune di Toceno è Titolare del trattamento ed ha individuato il Responsabile della prevenzione della corruzione e della trasparenza (c.d. RPCT) competente a gestire le segnalazioni pervenute attraverso il canale di segnalazione interna.
L'RPCT, incarico ricoperto negli enti locali dal segretario comunale, sarà autorizzato al trattamento dei dati con apposita lettera redatta ai sensi dell'art. 29 GDPR.
Il Comune, inoltre, si avvarrà di un soggetto esterno che fornisce la piattaforma di segnalazione e gestione degli illeciti. In particolare, tale soggetto, Whistleblowing Solutions Impresa Sociale S.r.l. (di seguito "Whistleblowing Solutions"), sarà nominato Responsabile del trattamento ai sensi dell'art. 28 GDPR in quanto si occuperà della gestione del sistema di whistleblowing per l'esecuzione di operazioni informatizzate di trattamento di dati personali relative alla raccolta e alla conservazione dei dati necessari per l'erogazione del servizio.
Il Responsabile del trattamento, Whistleblowing Solutions, si avvale di altri soggetti esterni per l'erogazione del servizio che ha nominato come Sub-Responsabili; tali soggetti sono Seeweb quale Sub-Responsabile del trattamento per la gestione dell'infrastruttura (IaaS) e Transparency International Italia quale Sub-Responsabile del trattamento per la collaborazione nella gestione del sistema di whistleblowing.

Ci sono standard applicabili al trattamento?
Whistleblowing Solutions, quale Responsabile del trattamento dei dati, ha acquisito le seguenti certificazioni:
- ISO27001 "Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks"
- ISO27017 controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud
- ISO27018 per la protezione dei dati personali nei servizi Public Cloud
- Qualifica AGID
- Certificazione CSA Star

3.2. Dati, processi e risorse di supporto

Quali sono i dati trattati?
- Dati di registrazione: Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (es. RPCT).
- Dati identificativi: dati anagrafici e di contatto del segnalante (qualora non si proceda con segnalazione anonima) e dati identificativi del segnalato e di altri soggetti citati nella segnalazione;
- Categorie particolari di dati: dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati;

- Dati relativi a condanne penali e reati: dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

Le segnalazioni 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.

Sono destinatari dei dati raccolti a seguito della segnalazione, se del caso, l'Autorità Giudiziaria, la Corte dei conti e l'ANAC. Inoltre, fra i destinatari vi rientra anche Whistleblowing Solutions quale fornitore del servizio di erogazione e gestione operativa della piattaforma tecnologica di digital whistleblowing in qualità di Responsabile del trattamento ai sensi dell'art. 28 GDPR e i Sub-Responsabili nominati da quest'ultimo.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?
Le segnalazioni possono pervenire, ed essere quindi raccolte, tramite la piattaforma digitale messa a disposizione dei segnalanti.
Per quanto riguarda le segnalazioni attraverso la piattaforma digitale il ciclo di vita del trattamento è il seguente:
1) Attivazione della piattaforma.
2) Configurazione della piattaforma.
3) Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi preposti.
4) Analisi della segnalazione e gestione da parte dell'RPCT attraverso indagini interne o richieste con adozione di provvedimenti conseguenti.
5) Chiusura di una segnalazione e conservazione fino al termine di 5 anni dalla comunicazione di chiusura.
6) Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge per finalità amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore.

Quali sono le risorse di supporto ai dati?
1) Software di whistleblowing professionale GlobaLeaks.
2) Infrastruttura IaaS e SaaS privata basata su tecnologie:
   - Dettaglio Hardware
   - VMWARE (virtualizzazione)
   - Debian Linux LTS (sistema operativo)
   - VEEAM (backup)
   - OPNSENSE (firewall)
   - OPENVPN (vpn)

4. Principi Fondamentali

4.1. Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?
Il trattamento dei dati riguardanti le persone che segnalano una violazione, le persone a cui la violazione è attribuita e gli altri soggetti eventualmente coinvolti è previsto da norme di legge che ne stabiliscono la finalità e la legittimità. In particolare, la L. 179/2017 e il D.lgs. 24/2023 sono volte a favorire il processo di segnalazione. Infatti, garantire la protezione dei soggetti che si espongono con segnalazioni, denunce o con l'istituto della divulgazione pubblica, contribuisce all'emersione e alla prevenzione di rischi e situazioni pregiudizievoli per la stessa amministrazione e, di riflesso, per l'interesse pubblico collettivo.

Quali sono le basi legali che rendono lecito il trattamento?
La base giuridica del trattamento dei dati personali degli interessati è individuabile nell'obbligo di legge (art. 6, lett. c) GDPR) previsto in capo al Titolare del trattamento, consistente nel dover prevenire rischi e situazioni

pregiudizievoli per l'interesse pubblico (art. 6, lett. e) GDPR) con danno, anche soltanto d'immagine, per l'Ente e nel dover individuare strumenti di tutela nei confronti dei lavoratori che denuncino reati o irregolarità di cui siano venuti a conoscenza nell'ambito delle proprie attività lavorative (L. 179/2017 e D.lgs. 24/2023).
Inoltre, la base giuridica che legittima la comunicazione dei dati personali del segnalante al segnalato nell'ambito del procedimento disciplinare, qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, è il consenso espresso della persona segnalante alla rivelazione della sua identità (art. 6, lett. a) GDPR).

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?
Per la registrazione e attivazione del servizio tramite piattaforma digitale sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, Email di ruolo dell'utente che effettua la registrazione del Comune sulla piattaforma e i dati relativi all'ente (nome, indirizzo, CF e PI).
Il software di whistleblowing raccoglie segnalazioni secondo i migliori questionari predisposti in ambito di whistleblowing in collaborazione con importanti enti di ricerca in materia di whistleblowing e anticorruzione e messi a punto da Transparency International Italia in relazione alla normativa vigente in materia.
Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo GlobaLeaks, log di sistema e firewall sono configurati per non registrare 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 GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

I dati sono esatti e aggiornati?
L'aggiornamento dei dati attraverso la piattaforma digitale messa a disposizione 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.
In ogni caso l'RPCT dà seguito ad una richiesta di rettifica o integrazione dei dati personali da parte del segnalante o degli altri soggetti secondo la procedura di gestione delle richieste di esercizio dei diritti privacy adottata dal Comune.

Qual è il periodo di conservazione dei dati?
Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario alla gestione delle stesse e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione (art. 14 D.Lgs. 24/2023).

Inoltre, la piattaforma digitale ha una policy di data retention di default delle segnalazioni di 12 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute.
La proroga della scadenza può essere fatta dal soggetto ricevente più volte.
Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio a condizione che non esistano segnalazioni aperte sulla piattaforma.

4.2. Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?
Il Comune di Toceno mette a disposizione dei soggetti interessati (segnalante, segnalato, altri soggetti coinvolti) apposita informativa privacy resa ai sensi dell'art. 13 GDPR nella sezione privacy e nella sezione dedicata alle segnalazioni di whistleblowing sul proprio sito internet istituzionale. In tale ultima sezione verranno, inoltre, resi disponibili la procedura adottata dall'ente, il link di collegamento alla piattaforma digitale per l'invio delle segnalazioni e le ulteriori indicazioni sulla gestione delle segnalazioni di whistleblowing.

Ove applicabile: come si ottiene il consenso degli interessati?
Per il trattamento dei dati relativi alla procedura di whistleblowing non è necessario raccogliere un consenso dell'interessato in quanto il trattamento ha quale base giuridica l'adempimento di un obbligo di legge a cui è soggetto il Titolare del trattamento.
Il D.Lgs. 24/2023 disciplina però due ipotesi in cui è necessario raccogliere il consenso del segnalante quale soggetto interessato:

1. La prima ipotesi ricorre laddove nell'ambito di un procedimento disciplinare avviato nei confronti del presunto autore della condotta segnalata, l'identità del segnalante risulti indispensabile alla difesa del soggetto cui è stato contestato l'addebito disciplinare. In tal caso, oltre al previo consenso del segnalante da raccogliere per iscritto è necessario anche comunicare, sempre previamente, in forma scritta a quest'ultimo le motivazioni che conducono al disvelamento della sua identità.
2. La seconda ipotesi ricorre, invece, nel caso in cui nelle procedure di segnalazione interna ed esterna la rivelazione dell'identità del segnalante sia indispensabile anche ai fini della difesa della persona coinvolta. Anche in questo caso per disvelare l'identità del segnalante è necessario acquisire previamente sia il consenso espresso dello stesso che notificare allo stesso, in forma scritta, le motivazioni alla base della necessità di disvelare la sua identità.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?
Il Comune di Toceno ha adottato una procedura di gestione delle richieste di esercizio dei diritti in materia di privacy e ha previsto la pubblicazione sul proprio sito istituzione nella sezione Privacy di un modulo con cui il soggetto interessato può esercitare i suoi diritti.
Nel dettaglio, il segnalante può esercitare il diritto accesso ai proprio dati rivolgendosi direttamente all'RPCT mentre i soggetti segnalati o altri soggetti coinvolti nella segnalazione (es. testimoni) possono esercitare, ai sensi dell'art. 2-undecies, lett. f) e parag. 3) del D.Lgs. 196/2003, tale diritto per il tramite del Garante Privacy con la modalità di cui all'art. 160 del D.Lgs. 196/2003.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?
Il Comune di Toceno ha adottato una procedura di gestione delle richieste di esercizio dei diritti in materia di privacy e ha previsto la pubblicazione sul proprio sito istituzione nella sezione Privacy di un modulo con cui il soggetto interessato può esercitare i suoi diritti. Nel dettaglio, il segnalante può esercitare il diritto di rettifica e cancellazione rivolgendosi direttamente all'RPCT mentre i soggetti segnalati o altri soggetti coinvolti nella segnalazione (es. testimoni) possono esercitare, ai sensi dell'art. 2-undecies, lett. f) e parag. 3) del D.Lgs. 196/2003, tali diritti per il tramite del Garante Privacy con la modalità di cui all'art. 160 del D.Lgs. 196/2003.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?
Il Comune di Toceno ha adottato una procedura di gestione delle richieste di esercizio dei diritti in materia di privacy e ha previsto la pubblicazione sul proprio sito istituzione nella sezione Privacy di un modulo con cui il soggetto interessato può esercitare i suoi diritti. Nel dettaglio, il segnalante può esercitare i diritti di limitazione e opposizione ai proprio dati rivolgendosi direttamente all'RPCT mentre i soggetti segnalati o altri soggetti coinvolti nella segnalazione (es. testimoni) possono esercitare, ai sensi dell'art. 2-undecies, lett. f) e parag. 3) del D.Lgs. 196/2003, tali diritti per il tramite del Garante Privacy con la modalità di cui all'art. 160 del D.Lgs. 196/2003.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?
Gli accordi contrattuali saranno definiti con le seguenti società:

- Whistleblowing Solutions in qualità di Responsabile del trattamento.
- Seeweb in qualità di Sub-Responsabile del trattamento nominato da Whistleblowing Solutions.
- Transparency International Italia in qualità di Sub-Responsabile del trattamento nominata da whistleblowing Solutions.

Ogni accordo disciplinerà in maniera puntale i rispettivi obblighi in materia di protezione dei dati personali.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?
I Dati Personali saranno trattati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Europea. Non esiste alcun trasferimento di dati personali verso paesi extra UE.

5. Rischi

5.1. Misure esistenti o pianificate

Crittografia
La piattaforma digitale utilizzata dal Comune di Toceno e fornita da Whistleblowing Solutions ha alla base l'applicativo GlobaLeaks che 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.
Protocollo crittografico: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html.

Controllo degli accessi logici
L'accesso all'applicativo è consentito ad ogni utilizzatore autorizzato (RPCT) 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.
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.

Vulnerabilità
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.
Audit di sicurezza: https://docs.globaleaks.org/en/main/security/PenetrationTests.html.

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 e 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 e 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
Il Comune di Toceno ha adottato una procedura di gestione dei data breach. Inoltre, anche il Responsabile del trattamento Whistleblowing Solutions ha definito una procedura per la gestione delle violazioni dei dati personali.

Lotta contro il malware
Tutti i computer del Comune di Toceno e del personale di Whistleblowing Solution 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.

Contratto con il responsabile del trattamento
Il Comune di Toceno sottoscriverà, ai sensi dell'art. 28 GDPR, apposito atto con il Responsabile del trattamento dei dati Whistleblowing Solutions al fine di disciplinare i rispettivi obblighi in materia di trattamento dei dati personali.

Politica di tutela della privacy
Il Comune di Toceno ha nominato un DPO esterno ai sensi dell'art. 37 GDPR che svolge i compiti stabiliti dall'art. 39 GDPR sulla base di un contratto di servizi.
Inoltre, il personale dipendente del Comune di Toceno svolge periodicamente una formazione in materia di protezione dei dati personali comprensiva anche dei rischi informatici ed è stato istruito rispetto al coretto trattamento dei dati.

5.2. Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Danno per la reputazione
Discriminazione
Perdita di controllo dei dati
Altri svantaggi economici e sociali
Impossibilità di esercitare diritti, servizi o opportunità

Quali sono le principali minacce che potrebbero concretizzare il rischio?
Errore umano
Attacchi informatici alla rete
Furto dei supporti fisici di archiviazione e registrazione

Quali sono le fonti di rischio?
Persona, interna o esterna al Comune o al Responsabile del trattamento
Virus informatici

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?
Crittografia
Controllo degli accessi logici
Tracciabilità
Sicurezza dei canali informatici
Sicurezza dell'hardware
Lotta contro il malware
Contratto con il responsabile del trattamento
Politica di tutela della privacy

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Massima.
L'Impatto per il segnalante è sicuramente alto in quanto lo stesso potrebbe essere discriminato e subire ritorsioni nel proprio contesto lavorativo a seguito della segnalazione effettuata se questa viene resa nota o accessibile a persone non autorizzate.
Anche il soggetto segnalato potrebbe avere degli impatti alti derivanti dalla diffusione del proprio nominativo quale potenziale autore di reato a maggior ragione qualora la segnalazione risulti poi non fondata.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Limitata.
Le misure implementate riducono la probabilità che l'evento si verifichi.

5.3. Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Danno per la reputazione.
Discriminazione.
Altri svantaggi economici e sociali.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?
Attacchi informatici alla rete.
Errore umano.

Quali sono le fonti di rischio?
Virus informatici.
Persona, interna o esterna al Comune o al Responsabile del trattamento.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Backup.
Crittografia.
Controllo degli accessi logici.
Tracciabilità.
Sicurezza dei canali informatici.
Sicurezza dell'hardware.
Lotta contro il malware.
Politica di tutela della privacy.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?
Importante.
L'Impatto per il segnalante è sicuramente importante in quanto i dati potrebbero non essere esatti e dunque determinare delle problematiche di comunicazione con l'RPCT oppure determinare degli errori nell'azione di verifica dell'RPCT conseguenti alla segnalazione.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?
Limitata.
Le misure implementate riducono la probabilità che l'evento si verifichi.

5.4. Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?
Impossibilità di esercitare diritti, servizi o opportunità.
Altri svantaggi economici e sociali.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?
Errore umano.
Attacchi informatici alla rete.
Furto dei supporti fisici di archiviazione e registrazione.

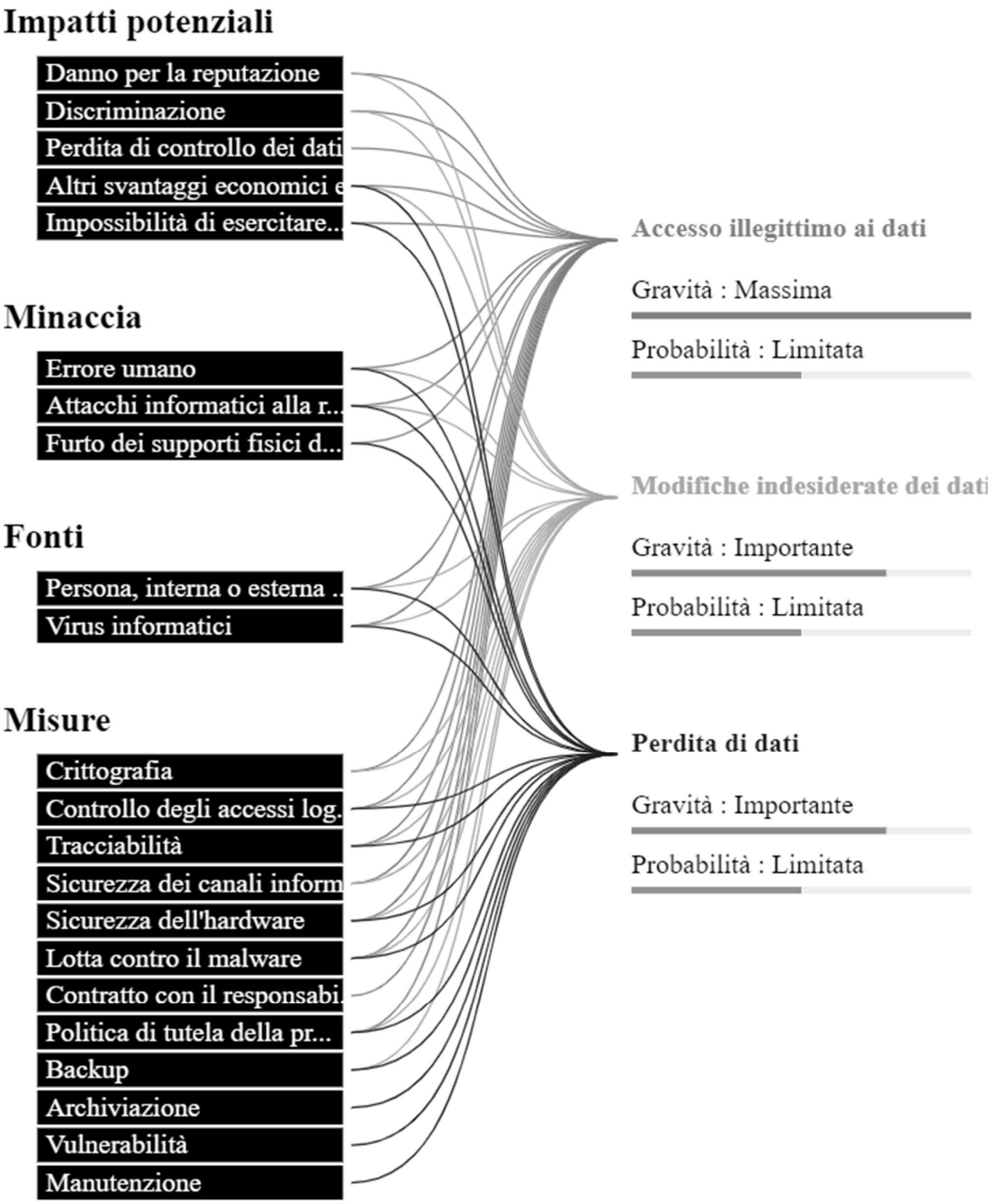
Quali sono le fonti di rischio?
Persona, interna o esterna al Comune o al Responsabile del trattamento.
Virus informatici.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Backup.
Controllo degli accessi logici.
Tracciabilità.
Archiviazione.
Vulnerabilità.
Manutenzione.
Sicurezza dell'hardware.
Lotta contro il malware.
Politica di tutela della privacy.

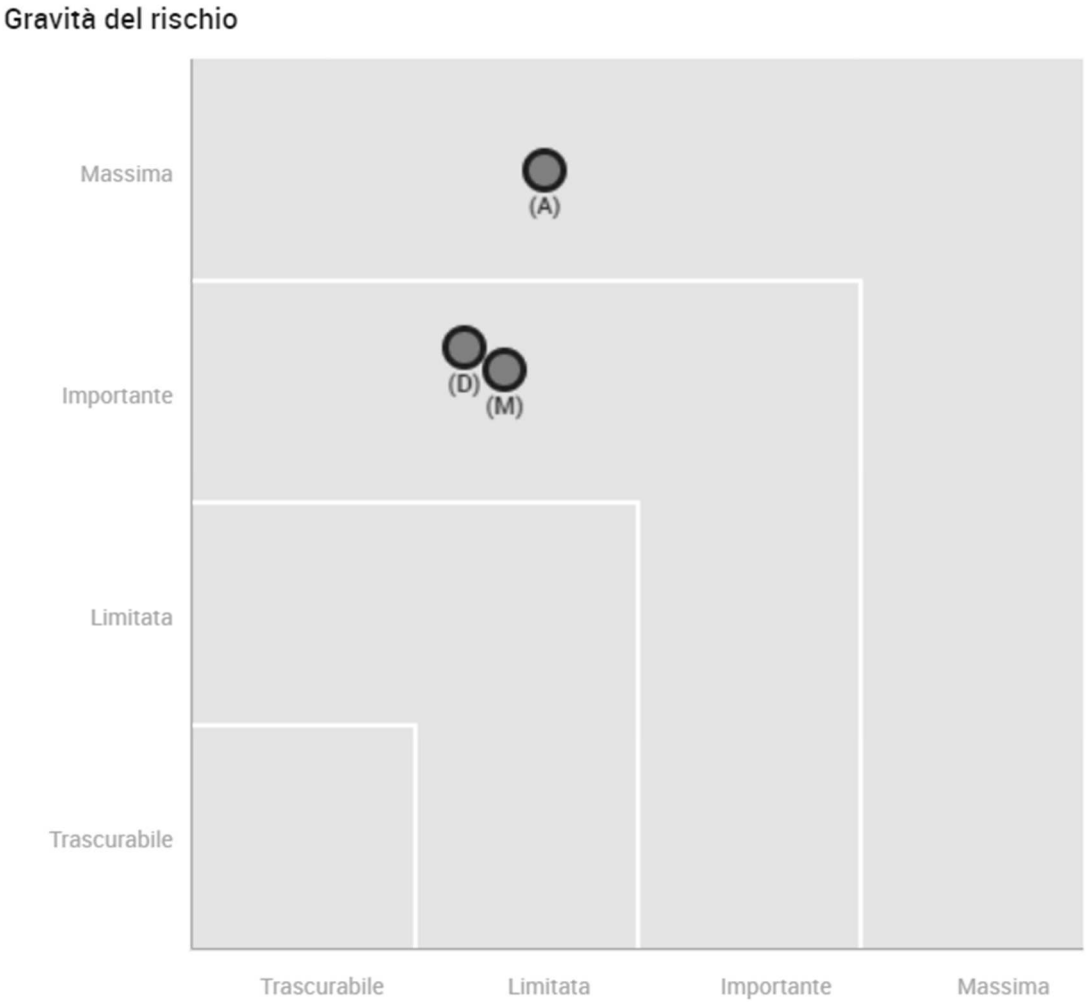
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Importante.
L'impatto per il segnalante è sicuramente importante in quanto lo stesso non potrebbe più esercitare i diritti a lui spettanti o la tutela prevista dalla normativa oltre che determinare l'impossibilità di procedere con le verifiche conseguenti alla segnalazione.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Limitata.
Le misure implementate riducono la probabilità che l'evento si verifichi.

5.5. Panoramica dei rischi



5.6. Valutazione del rischio



- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

6. Parere del DPO e degli interessati

Parere del DPO:
Le misure di sicurezza previste consentono di operare ai sensi della normativa rispettando la riservatezza del segnalante, del segnalato e degli eventuali soggetti terzi. Il trattamento essendo previsto per legge può essere svolto nelle modalità analizzate.

Richiesta del parere degli interessati
Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati
Il trattamento oggetto di valutazione potenzialmente coinvolge un numero non definito e una tipologia di interessati vari e, pertanto, è impossibile richiederne un parere.

7. Conclusioni

Dopo aver valutato nel dettaglio quanto richiesto dal par. 7 dell'art. 35 GDPR, il Comune può concludere che il trattamento dei dati relativo alle ricezione e gestione delle segnalazioni di whistleblowing analizzato risulta:

1) **Proporzionato** alla finalità previste da normativa: le misure poste a protezione dei dati personali dei soggetti coinvolti nel procedimento di whistleblowing consente di ritenere il trattamento proporzionato rispetto ai diritti e alle libertà dei soggetti interessati.
2) È **necessario**, in quanto tale finalità è prevista da legge nel rispetto di adeguate misure di sicurezza poste a protezione dei dati personali degli interessati.