COMUNE DI TORRI IN SABINA

PROVINCIA DI RIETI

Data revisione	28/08/2026

Sommario

1. DATI IDENTIFICATIVI DEL DOCUMENTO

Titolare del trattamento	Comune di Torri in Sabina (Provincia di Rieti)
DPO	dpo@basicsrl.com
Responsabile del trattamento	Whistleblowing Solutions S.r.l.
Oggetto del trattamento	Dati personali relativi a segnalazioni di illeciti (whistleblowing)
Base normativa	Art. 35 GDPR; D.Lgs. 24/2023; ANAC Delibera n. 478/2025
Ufficio competente	RPCT / Ufficio Whistleblowing

2. NECESSITÀ DELLA DPIA

2.1 Valutazione preliminare

Ai sensi dell'Art. 35 GDPR, il Titolare del trattamento è tenuto a effettuare una valutazione d'impatto sulla protezione dei dati prima di procedere a qualsiasi trattamento di dati personali che comporti rischi elevati per i diritti e le libertà delle persone.

La presente DPIA è redatta per il trattamento dati relativo al sistema di whistleblowing implementato dal Comune di Torri in Sabina in ottemperanza al D.Lgs. 24/2023 (attuazione della Direttiva UE 2019/1937).

2.2 Criteri che rendono la DPIA necessaria

La DPIA è **obbligatoria** per il presente trattamento in quanto ricorrono i seguenti fattori di rischio:

1. **Uso di nuove tecnologie**: piattaforma informatica crittografata online per raccolta segnalazioni (Art. 35(1) GDPR)
2. **Monitoraggio sistematico**: raccolta e analisi sistematica di informazioni relative a violazioni riscontrate nell'attività lavorativa
3. **Dati sensibili potenziali**: le segnalazioni possono contenere dati di categorie particolari (Art. 9 GDPR), inclusi dati sulla salute, convinzioni politiche, sindacalizzazione, condanne penali
4. **Ambito applicativo ampio**: il procedimento copre una gamma molto vasta di potenziali segnalanti (dipendenti, collaboratori, fornitori, volontari, stakeholder, ex dipendenti, soggetti in fase di selezione)
5. **Rischi agli interessati**: potenziale identificazione nonostante anonimato tecnico, discriminazione, ritorsione, danno reputazionale, perdita economica, danno psicologico
6. **Raccordo con diritti fondamentali**: bilanciamento tra diritto della persona a segnalare illeciti (protezione D.Lgs. 24/2023) e diritti della persona segnalata (diritto di difesa, reputazione)

2.3 Consultazione preventiva dell'Autorità

Secondo l'Art. 35(4) GDPR, il Titolare del trattamento deve consultare l'Autorità Garante per la protezione dei dati personali quando dalla DPIA emerge che il rischio non può essere efficacemente mitigato attraverso misure organizzative e tecniche.

Esito della valutazione preliminare: la consultazione preventiva **non è ritenuta necessaria** in quanto:

- Whistleblowing Solutions ha implementato misure di sicurezza e privacy by design conformi allo stato dell'arte (certificazioni ISO27001:2022, ISO27017:2015, ISO27018:2025, ISO9001:2015, CSA STAR Level 1)
- La procedura di gestione delle segnalazioni è stata redatta in conformità al D.Lgs. 24/2023 e alle Linee guida ANAC n. 478/2025
- Il rischio residuo è gestibile attraverso misure organizzative integrative da implementare a livello del Comune
- La documentazione della presente DPIA dimostra adeguatamente l'approccio accountability del Titolare

Tuttavia, il Titolare rimane libero di sottoporre la presente DPIA all'Autorità Garante per parere facoltativo secondo le modalità previste dall'Art. 35(9) GDPR.

3. DESCRIZIONE DEL TRATTAMENTO

3.1 Finalità del trattamento

Le finalità del trattamento sono:

1. **Gestione delle segnalazioni di illeciti**: raccolta, conservazione e elaborazione delle informazioni relative a violazioni riscontrate nel contesto dell'attività della Pubblica Amministrazione, ai sensi del D.Lgs. 24/2023
2. **Accertamento dei fatti segnalati**: svolgimento dell'istruttoria per verificare la fondatezza delle segnalazioni ricevute
3. **Comunicazione dell'esito**: informazione alla persona segnalante circa l'esito delle attività di accertamento
4. **Protezione dei segnalanti**: tutela dell'identità della persona segnalante e dei soggetti menzionati nella segnalazione, protezione contro ritorsioni e discriminazioni
5. **Conformità normativa**: adempimento degli obblighi derivanti dal D.Lgs. 24/2023 e dalle Linee guida ANAC
6. **Sicurezza dell'informazione**: monitoraggio della sicurezza della piattaforma mediante dati tecnici (log, diagnostica, statistiche anonimizzate)

3.2 Legittimità del trattamento

Il trattamento è legittimato da:

- **Art. 6(1)(c) GDPR**: adempimento di un obbligo legale (D.Lgs. 24/2023, artt. 1, 2, 3, 4, 5)
- **Art. 6(1)(e) GDPR**: esecuzione di un compito di interesse pubblico dell'Amministrazione (prevenzione della corruzione, trasparenza, legalità)
- **Art. 9(2)(h) GDPR**: trattamento di dati sensibili necessario per scopi di medicina del lavoro, valutazione della capacità lavorativa, per fini di medicina preventiva o occupazionale (per quanto attiene a segnalazioni su salute e sicurezza nei luoghi di lavoro)
- **Art. 10 GDPR**: trattamento di dati relativi a condanne penali e reati qualora necessario nel contesto della procedura whistleblowing

3.3 Titolari, Responsabili e Sub-Responsabili del trattamento

Ruolo	Soggetto	Competenze
Titolare	Comune di Torri in Sabina	Decisioni sulla liceità e finalità del trattamento
Responsabile	Whistleblowing Solutions S.r.l.	Gestione infrastruttura piattaforma GlobaLeaks, raccolta dati, conformità tecnica
Sub-Responsabile (Infrastruttura)	Seeweb S.r.l.	Gestione datacenter, hosting IaaS, backup, disaster recovery
Sub-Responsabile (Governance)	Transparency International Italia	Collaborazione gestione piattaforma, conformità procedurali
Ricevente dati	RPCT / Ufficio Whistleblowing (Comune)	Ricezione segnalazioni, accertamento, comunicazione esiti

Tutti i soggetti operano nel rispetto dei Contratti di trattamento dati (Data Processing Agreements) e della presente DPIA.

3.4 Categorie di interessati

Le categorie di interessati sono:

1. **Persone segnalanti** (Art. 2, D.Lgs. 24/2023):Dipendenti dell'Ente, Collaboratori e consulenti, Fornitori, subfornitori e loro dipendenti/collaboratori, Liberi professionisti, consulenti, lavoratori autonomi, Volontari e tirocinanti, Azionisti, amministratori, revisori, direttori, Ex dipendenti e ex collaboratori, Soggetti in fase di selezione
2. **Persone segnalate** (potenziali autori degli illeciti):Dipendenti dell'EnteAmministratori, dirigenti, funzionari, Soggetti indicati come responsabili di violazioni
3. **Altre persone menzionate nelle segnalazioni**: Testimoni, Soggetti coinvolti indirettamente, Vittime di illeciti
4. **Facilitatori** (Art. 3, D.Lgs. 24/2023):Persone che assistono la persona segnalante nel processo di segnalazione

3.5 Categorie di dati personali trattati

A) Dati comuni (Art. 4(1) GDPR)

1. **Dati di registrazione e contatto della persona segnalante**: Nome, Cognome, Ruolo professionale/status relativo all'Ente, Numero di telefono, Indirizzo email
2. **Dati di identificazione dell'Ente**: Nome, indirizzo, codice fiscale, partita IVA dell'ente
3. **Dati identificativi delle persone menzionate**: Nome, Cognome, qualifica, ruolo della persona segnalata, Dati identificativi di altri soggetti menzionati nella segnalazione
4. **Contenuto della segnalazione**: Descrizione degli illeciti sospetti. Fatti, circostanze, date Riferimenti a fonti di conoscenza Documenti allegati (potenzialmente illimitati)

B) Dati di categorie particolari (Art. 9 GDPR)

Le segnalazioni possono potenzialmente contenere dati appartenenti alle categorie particolari di cui all'Art. 9:

1. **Dati sulla salute**: segnalazioni relative a violazioni in materia di salute e sicurezza nei luoghi di lavoro (D.Lgs. 81/2008), malattie professionali, infortuni
2. **Dati su convinzioni politiche, religiose, sindacali**: segnalazioni di discriminazioni basate su appartenenza sindacale, convinzioni politiche, religiose
3. **Dati relativi a condanne penali e reati** (Art. 10 GDPR): segnalazioni di comportamenti potenzialmente costituenti reato

C) Dati tecnici per sicurezza dell'informazione

1. **Log applicativi**:Timestamp transazioni, ID sessione (non correlato a IP o User Agent del segnalante), Azioni effettuate sulla piattaforma, Errori e eccezioni
2. **Informazioni diagnostiche**: Versione software, Stato della piattaforma, Risultati controlli di integrità
3. **Dati statistici anonimizzati**: Numero segnalazioni per periodo, Tipologie di illeciti segnalati, Tempi medi di gestione

3.6 Periodo di conservazione

Categoria di dati	Periodo di conservazione	Base normativa
Segnalazioni aperte	Fino a completamento accertamento	Necessità funzionale
Segnalazioni chiuse	Massimo 12 mesi (policy di default)	Art. 5(1)(e) GDPR (limitazione conservazione)
Estensione conservazione	Fino a 3 mesi oltre scadenza 12 mesi (su richiesta RPCT)	Necessità accertamenti ulteriori
Massimale temporale	5 anni dal comunicazione esito accertamento	Prescrizione amministrativa, contabile
Conservazione obbligatoria	Per segnalazioni trasferite a Procura/Corte Conti	Termini processuali
Cancellazione piattaforma	15 giorni dopo disattivazione servizio (se nessuna segnalazione aperta)	Operativa di chiusura
Log di audit	Massimo 5 anni (eccetto log pertinenti segnalazioni conservate)	Tracciabilità amministrativa

La retention policy è configurabile a livello di piattaforma dal RPCT in base alle necessità organizzative, nel rispetto dei termini massimi stabiliti.

3.7 Destinatari dei dati

I dati personali trattati sono comunicati a:

1. **Interno al Comune**: RPCT (Responsabile Prevenzione Corruzione e Trasparenza)
2. **Esterno al Comune (quando necessario)**:Procura della Repubblica (Art. 331 c.p.p., se reato configurato), Corte dei Conti (in caso di danno erariale), Autorità Nazionale Anticorruzione (in caso di segnalazione esterna ai sensi D.Lgs. 24/2023), Organi di controllo (ANAC, Autorità giudiziaria)
3. **Processore e Sub-processori**: Whistleblowing Solutions (accesso ai dati come Responsabile del trattamento), Seeweb (accesso limitato a livello infrastrutturale), Transparency International Italia (accesso limitato per governance)

Limitazione: I dati personali identificativi della persona segnalata non sono inclusi nella comunicazione dell'esito al segnalante, conformemente al principio di riservatezza e proporzionalità.

4. ANALISI E VALUTAZIONE DEI RISCHI

4.1 Metodologia di valutazione

La presente DPIA utilizza la metodologia di risk assesment basata su:

- **Probabilità**: probabilità dell'evento avverso
- **Impatto**: gravità del danno per gli interessati
- **Rischio residuo**: determinato dalla combinazione probabilità × impatto, al netto delle misure di mitigazione già implementate

Scala di valutazione:

Livello	Descrizione
Basso	Probabilità e/o impatto ridotti; gestibile con misure standard
Medio	Probabilità e/o impatto moderati; richiede misure specifiche di mitigazione
Alto	Probabilità e/o impatto elevati; richiede misure organizzative e tecniche robuste
Critico	Rischio inaccettabile; può determinare violazione diritti fondamentali

4.2 Mapping dei rischi

4.2.1 RISCHIO R1: Identificazione involontaria della persona segnalante

Descrizione: Nonostante l'uso di tecnologie di protezione (crittografia, no-log, accesso via Tor), la persona segnalante potrebbe essere identificata attraverso:

- Correlazione dei metadati della segnalazione con altre informazioni
- De-anonimizzazione attraverso analisi del contenuto della segnalazione
- Errore umano durante accertamento o comunicazione con ricevente
- Accesso non autorizzato alla piattaforma

Interessati coinvolti: Persona segnalante, facilitatore, soggetto segnalato, altri menzionati

Probabilità: MEDIA (il sistema implementa misure robuste, ma il rischio di correlazione rimane in contesti piccoli)

Impatto: ALTO (perdita di protezione, rischio discriminazione, danno reputazionale, danno economico)

Rischio prima mitigazione: MEDIO-ALTO

Misure di mitigazione già implementate:

- Crittografia end-to-end con protocollo specifico per whistleblowing
- No cookie, no persistent storage lato client
- Accesso via Tor Browser per anonimato di rete
- Audit log privacy-preserving (no IP, no User Agent)
- Configurazione "no-log" della piattaforma
- Formazione dei riceventi su riservatezza
- Divieto di identificazione senza consenso esplicito (Art. 7, D.Lgs. 24/2023)

Misure di mitigazione aggiuntive da implementare (da parte del Titolare del Trattamento):

1. Procedura organizzativa: limitare circolazione informazioni durante accertamento a staff ristretto
2. Anonimizzazione preventiva: condividere con altre funzioni dell'Ente solo dati anonimizzati sulla segnalazione
3. Formazione RPCT/staff: sensibilizzazione su rischi de-anonimizzazione in contesti piccoli
4. Protocollo di accertamento: interviste separate, evitare confronti diretti segnalante-segnalato
5. Comunicazione cautela: esito fornito solo mediante piattaforma, con linguaggio neutrale

Rischio residuo: **MEDIO** (gestibile attraverso misure organizzative)

Monitoraggio: Revisione annuale della procedura; feedback da segnalanti

4.2.2 RISCHIO R2: Discriminazione e ritorsione contro il segnalante

Descrizione: La persona segnalante, una volta identificata (volontariamente o involontariamente), subisce:

- Discriminazione nel lavoro (trasferimento, riduzione orario, mancata promozione)
- Ritorsione diretta (licenziamento, sospensione)
- Ritorsione psicologica (mobbing, isolamento, pressione morale)
- Danno alla reputazione professionale
- Perdite economiche

Interessati coinvolti: Persona segnalante

Probabilità: **MEDIA** (il D.Lgs. 24/2023 proibisce la discriminazione, ma la pressione organizzativa persiste)

Impatto: **ALTO** (coinvolge diritti fondamentali quali occupazione, dignità, reputazione)

Rischio prima mitigazione: **MEDIO-ALTO**

Misure di mitigazione già implementate:

- Art. 2, D.Lgs. 24/2023: divieto di ritorsione e discriminazione
- Art. 4, D.Lgs. 24/2023: protezione facilitatori
- Art. 6, D.Lgs. 24/2023: sanzioni amministrative per ritorsioni (irrogate da ANAC)
- Canale esterno ANAC: salvaguardia in caso di rischio interno

Misure di mitigazione aggiuntive da implementare (da parte del Titolare del Trattamento):

1. Monitoraggio della ritorsione: RPCT raccoglie eventuali segnalazioni di discriminazione post-whistleblowing
2. Protezione temporale: garanzie specifiche per il periodo di accertamento e 2 anni successivi
3. Documentazione: registrazione di qualsiasi tentativo di ritorsione riscontrato
4. Escalation: segnalazione ad ANAC in caso di ritorsioni sospette

Rischio residuo: **MEDIO** (la protezione normativa esiste, ma l'enforcement dipende dalla vigilanza dell'Ente)

Monitoraggio: Verifica annuale presso RPCT; raccolta feedback segnalanti

4.2.3 RISCHIO R3: Violazione della riservatezza dei dati durante l'accertamento

Descrizione: Divulgazione involontaria o negligente di informazioni riservate della segnalazione a soggetti non autorizzati durante:

- Condivisione con altri uffici per accertamenti
- Comunicazione dell'esito
- Trasferimento a Procura/Corte Conti
- Storage temporaneo di documenti allegati

Interessati coinvolti: Persona segnalante, segnalato, altri menzionati

Probabilità: **MEDIA** (dipende dal comportamento organizzativo, non dalla tecnologia)

Impatto: **ALTO** (violazione confidenzialità, rischi di ritorsione, danno reputazionale)

Rischio prima mitigazione: **MEDIO-ALTO**

Misure di mitigazione già implementate:

- Crittografia end-to-end sulla piattaforma
- Accesso ristretto al RPCT e staff designato
- Divieto di stampa/condivisione non autorizzata
- Comunicazione esito senza dati personali segnalato

Misure di mitigazione aggiuntive da implementare (da parte del Titolare del Trattamento):

1. Protocollo di condivisione: preventiva anonimizzazione dei dati prima di comunicazione ad altri uffici
2. Accordi interni: formalizzare obbligo riservatezza per staff coinvolto in accertamenti
3. Documento sensitivo: marcare documenti con contrassegno "Riservato - Whistleblowing"
4. Gestione documentale: archiviare in fascicolo separato con accesso ristretto
5. Comunicazione all'esterno: coinvolgere DPO/RPCT per valutazione preliminare
6. Controllo di audit: spot check periodici su gestione documentale

Rischio residuo: **MEDIO** (gestibile attraverso procedure organizzative rigorose)

Monitoraggio: Audit interno annuale; controllo di conformità al protocollo

4.2.4 RISCHIO R4: Accesso non autorizzato alla piattaforma

Descrizione: Un soggetto non autorizzato accede ai dati della piattaforma whistleblowing mediante:

- Compromissione credenziali RPCT/staff
- Exploit vulnerabilità software
- Attacco esterno (brute force, injection, DDoS)
- Errore di configurazione della VPN/firewall
- Furto fisico di credenziali

Interessati coinvolti: Tutte le persone i cui dati sono sulla piattaforma

Probabilità: **BASSA** (il sistema implementa misure di sicurezza robuste; certificazione ISO27001)

Impatto: **CRITICO** (compromissione di tutte le segnalazioni, identificazione di massa, ritorsioni organizzate)

Rischio prima mitigazione: **MEDIO**

Misure di mitigazione già implementate:

- Autenticazione a due fattori (TOTP RFC 6238)
- Policy password sicura con divieto riutilizzo
- Accesso amministrativo via VPN

- Full Disk Encryption su server Linux
- Firewall perimetrale con VLAN segregate
- Audit log centralizzato
- Backup remoto con frequenza 8 ore
- Certificazione ISO27001:2022 con audit annuale
- Penetration test pubblici
  https://docs.globaleaks.org/en/stable/security/PenetrationTests.html

Misure di mitigazione aggiuntive da implementare (da parte del Titolare del Trattamento):

1. Gestione credenziali: password cambiate ogni 90 giorni per RPCT
2. Incident response: procedura di notifica rapida in caso di sospetta violazione
3. Formazione staff: training su phishing, social engineering, physical security

Rischio residuo: **BASSO** (misure tecniche robuste + controllo organizzativo)

Monitoraggio: Revisione semestrale dei log di accesso

4.2.5 RISCHIO R5: Dati sensibili non previsti nel contenuto della segnalazione

Descrizione: La segnalazione contiene dati di categorie particolari (Art. 9 GDPR) non anticipati:

- Informazioni su salute della persona segnalante/segnalata
- Dati genetici, biometrici
- Dati su convinzioni sindacali, politiche, religiose
- Dati su vita sessuale, orientamento sessuale
- Dati relativi a condanne penali, reati non denunciati

Questi dati, pur rilevanti per la segnalazione, sono trattati in base alla eccezione del D.Lgs. 24/2023 (interesse pubblico alla prevenzione della corruzione), ma richiedono safeguard aggiuntivi.

Interessati coinvolti: Segnalante, segnalato, altri menzionati

Probabilità: **MEDIA** (dipende dalla natura degli illeciti segnalati; es. segnalazioni su discriminazione sindacale implicheranno dati sensibili)

Impatto: **ALTO** (i dati sensibili hanno protezione rafforzata; rischio di trattamento illegittimo)

Rischio prima mitigazione: **MEDIO-ALTO**

Misure di mitigazione già implementate:

- Base legale Art. 9(2)(h) GDPR per dati salute/medicina del lavoro
- Base legale Art. 10 GDPR per dati su condanne penali
- Crittografia end-to-end della segnalazione
- No trattamento automatizzato o profilazione
- Raccordo con D.Lgs. 81/2008 (prevenzione infortuni, malattie professionali)

Misure di mitigazione aggiuntive da implementare (titolare del trattamento):

1. Informativa specifica: quando RPCT identifica dati sensibili, applicare informativa Art. 14 GDPR alla persona interessata (con ritardo se compromette accertamento)
2. Minimizzazione attiva: nel redigere accertamento, eliminare dati sensibili non strettamente necessari
3. Pseudonimizzazione: laddove possibile, riferirsi a persone mediante codice numerico invece di identità
4. Accesso ristretto: consentire accesso ai dati sensibili solo al RPCT, non allo staff di supporto
5. Audit annuale: verificare se segnalazioni contenevano dati sensibili e se appropriatamente protetti
6. Cancellazione accelerata: rimuovere dati sensibili prima della scadenza 12 mesi se non più necessari

Rischio residuo: **MEDIO** (gestibile attraverso cautela nella manipolazione dati)

Monitoraggio: Audit annuale; feedback RPCT

4.2.6 RISCHIO R6: Conservazione dati oltre il necessario

Descrizione: Le segnalazioni vengono conservate oltre i termini stabiliti (12 mesi + estensioni) per:

- Negligenza amministrativa (dimenticanza dell'RPCT)
- Ambiguità sulla scadenza
- Cumulo di conservazione legale (termini prescrizione, contabili)
- Mancata cancellazione automatica della piattaforma

Interessati coinvolti: Tutte le persone i cui dati sono nelle segnalazioni

Probabilità: **MEDIA** (il rischio è principalmente organizzativo, non tecnico)

Impatto: **MEDIO** (violazione Art. 5(1)(e) GDPR, ma non causa danno diretto agli interessati)

Rischio prima mitigazione: **MEDIO**

Misure di mitigazione già implementate:

- Policy di default 12 mesi configurata sulla piattaforma
- Cancellazione automatica sicura al raggiungimento della scadenza
- Estensione manuale: RPCT decide se prorogare (con tracciamento)
- Procedura Comune: esplicito divieto di conservazione oltre scadenza
- 15 giorni dopo disattivazione servizio: cancellazione piattaforma (se nessuna segnalazione aperta)

Misure di mitigazione aggiuntive da implementare (Comune):

1. Calendario di scadenza: RPCT mantiene registro delle segnalazioni e loro scadenze (in formato anonimizzato)
2. Reminder automatico: 1 mese prima della scadenza, notifica al RPCT per valutazione estensione
3. Revisione annuale: audit sulla compliance con retention policy
4. Documentazione: conservare traccia di ogni decisione di estensione (con motivazione)
5. Trasferimento legale: se segnalazione trasferita a Procura, interrompere countdown retention su piattaforma Comune

Rischio residuo: **BASSO** (gestibile con procedure amministrative semplici)

Monitoraggio: Revisione annuale della retention; audit di conformità

4.2.7 RISCHIO R7: Violazione della riservatezza durante trasferimento a Procura/Corte Conti

Descrizione: Nel momento in cui la segnalazione è trasferita a autorità esterne (Procura della Repubblica, Corte dei Conti, ANAC):

- Rischio che l'identità del segnalante sia rivelata ai soggetti indagati
- Violazione dell'anonimato prima della necessità processuale
- Esposizione a ritorsioni durante fase investigativa
- Divulgazione prematura a soggetti non autorizzati

Interessati coinvolti: Persona segnalante, segnalato

Probabilità: **MEDIA** (il trasferimento è necessario, ma il timing/modalità sono critici)

Impatto: **ALTO** (rischio ritorsione, danno reputazionale, compromise investigazione)

Rischio prima mitigazione: **MEDIO-ALTO**

Misure di mitigazione già implementate:

- Art. 8, D.Lgs. 24/2023: condizioni per trasferimento a Procura/Corte Conti
- Comunicazione al segnalante: notifica quando identità sarà resa nota

Misure di mitigazione aggiuntive da implementare (Titolare del Trattamento):

1. Comunicazione preventiva: informare segnalante 48 ore prima del trasferimento (salvo urgenza)
2. Modalità trasferimento: comunicare tramite piattaforma per mantenere canale sicuro
3. Documentazione: conservare copia della comunicazione al segnalante e data effettivo trasferimento
4. Valutazione preliminare: RPCT valuta se trasferimento a Procura è necessario PRIMA di inoltrare
5. Anonimizzazione parziale: trasferire con identità anonimizzata se permesso dalla natura del reato
6. Protezione temporale: comunicare al segnalante quando diritto di difesa entrerà in gioco (se mai)

Rischio residuo: **MEDIO** (gestibile attraverso coordinamento procedurale)

Monitoraggio: Tracciamento di ogni trasferimento; feedback segnalanti

4.2.8 RISCHIO R8: De-anonimizzazione attraverso analisi del contenuto della segnalazione

Descrizione: Nonostante i metadati siano protetti, la persona segnalante potrebbe essere identificata attraverso analisi del contenuto della segnalazione:

- Dettagli altamente specifici che identificano univocamente l'autore
- Stile di scrittura
- Correlazione con eventi conosciuti interni all'Ente
- Numero ristretto di dipendenti che conosce certi dettagli

Questo rischio è particolarmente acuto in enti piccoli (come un Comune).

Interessati coinvolti: Persona segnalante

Probabilità: **MEDIA-ALTA** (in contesti piccoli, il rischio è non trascurabile)

Impatto: **ALTO** (compromissione anonimato, rischio ritorsione)

Rischio prima mitigazione: **MEDIO-ALTO**

Misure di mitigazione già implementate:

- Questionario strutturato: guidance sulla segnalazione per evitare dettagli non necessari

- Assenza di metadati: no timestamp, localizzazione

Misure di mitigazione aggiuntive da implementare (Comune):

1. Guidance al segnalante: sulla piattaforma, consiglio di evitare dettagli altamente personali/specifici
5. Review RPCT: prima di accertamento, valutare se contenuto è troppo specifico e comporta rischio di-anonimizzazione
6. Comunicazione esito: evitare di riciclare frasi dalla segnalazione originale nella comunicazione
7. Consiglio di anonimato: consigliare al segnalante, se previsto, di rimanere anonimo se il contenuto identifica troppo facilmente

Rischio residuo: **MEDIO** (impossibile eliminarsi totalmente in contesti piccoli; gestibile attraverso cautela)

Monitoraggio: Valutazione caso-per-caso da parte RPCT

4.3 Tabella riepilogativa dei rischi

Rischio	Descrizione	Probabilità	Impatto	Residuo	Mitigazione
R1	Identificazione segnalante	Media	Alto	Medio	Organizz. + Tecn.
R2	Discriminazione/ritorsione	Media	Alto	Medio	Organizz.
R3	Violazione riservatezza	Media	Alto	Medio	Organizz.
R4	Accesso non autorizzato	Bassa	Critico	Medio	Tecniche
R5	Dati sensibili non previsti	Media	Alto	Medio	Organizz.
R6	Retenzione oltre termine	Media	Medio	Basso	Organizz.
R7	Violazione trasferimento esterno	Media	Alto	Medio	Organizz.
R8	De-anonimizzazione contenuto	Media-Alta	Alto	Medio	Organizz.

Conclusione: Tutti i rischi residui sono valutati come **MEDIO** o **BASSO**; quindi, gestibili attraverso misure organizzative e tecniche già implementate o da implementarsi. Non emerge rischio CRITICO che giustifichi blocco del trattamento.

5. MISURE ORGANIZZATIVE E TECNICHE DI MITIGAZIONE

5.1 Misure *tecniche già implementate (a cura di Whistleblowing Solutions)*

Crittografia

- **Transito dati**: TLS 1.2+ con rating A+ SSLLabs
- **Dati a riposo**: Crittografia end-to-end con chiave asimmetrica personale (curve ellittiche)
- **Full Disk Encryption**: su server Linux (lvm/crypto)
- **Protocollo specifico**: GlobaLeaks whistleblowing encryption protocol https://docs.globaleaks.org/en/stable/technical/security/encryption-protocol.html

Controllo accessi

- **Autenticazione**: Credenziali personali obbligatorie
- **2FA**: TOTP secondo RFC 6238
- **Password**: policy sicura con divieto riutilizzo
- **Accesso amministrativo**: VPN + SSH
- **Audit log**: centralizzato, privacy-preserving

Privacy by design

- **No cookie**: assenza totale di tracking cookie
- **No persistent storage**: sessioni temporanee solo
- **No IP logging**: audit log non contiene IP del segnalante
- **Accesso via Tor**: supporto Tor Browser per anonimato rete

Archiviazione sicura

- **Database SQLite**: acceduto tramite ORM con controllo applicativo
- **Controllo retention**: policy configurabile, cancellazione sicura
- **Backup remoto**: frequenza 8 ore, RPO 8 ore, policy retention 7 giorni

Infrastruttura

- **Hosting**: Datacenter Seeweb ISO27001, con monitoring 7x24, videosorveglianza, controllo accessi fisici
- **Firewall**: perimetrale + segregazione VLAN
- **High Availability**: cluster ridondante (2 firewall, 2 server fisici)
- **KMS**: Key Management System per continuità servizio

Manutenzione e vulnerabilità

- **Audit annuale**: security audit indipendenti pubblicati
- **Penetration test**: pubblici, risultati online
- **Peer review**: dalla comunità open-source
- **Patching**: procedure regolari di aggiornamento

5.2 Misure organizzative da implementare (a cura del Titolare del Trattamento)

A) Governance e responsabilità

1. **Designazione RPCT**: formale nomina del Responsabile Prevenzione Corruzione e Trasparenza come gestore segnalazioni
2. **Staff di supporto**: se previsto, designazione scritta di personale autorizzato ad accedere ai dati
3. **Accordi di riservatezza**: tutti gli operatori firmano clausola confidenzialità
4. **Accountability**: tracciamento di chi accede ai dati e quando

B) Procedure di sicurezza e riservatezza

1. **Accesso al sistema**: Password cambiate ogni 90 giorni, nessuna condivisione di credenziali, Logout automatico dopo inattività, Monitoraggio semestrale dei log di accesso
2. **Gestione della segnalazione**: Ricevuta automatica al segnalante (entro 7 giorni), Riscontro sull'accertamento (entro 3 mesi), Comunicazione esito senza dati personali segnalato, Cartella riservata separata per segnalazioni whistleblowing
3. **Condivisione dati interni**: Preventiva anonimizzazione quando comunicate ad altri uffici, Documento marchiato "Riservato - Whistleblowing", Accesso ristretto a personale con esigenza diretta, Tracciamento di accessi/condivisioni
4. **Trasferimento a Procura/Corte Conti**: Valutazione preliminare RPCT, Comunicazione al segnalante 48 ore prima (salvo urgenza), Conservazione copia comunicazione, Aggiornamento status segnalazione su piattaforma

C) Formazione e sensibilizzazione

1. **RPCT e staff**: Training annuale su D.Lgs. 24/2023, GDPR, rischi de-anonimizzazione, Sensibilizzazione su divieto discriminazione/ritorsione, Procedura di escalation per sospette ritorsioni
2. **Dipendenti (comunicazione generale)**:Informativa sul sistema whistleblowing, Tolleranza zero verso ritorsioni, Canali disponibili (interno + esterno ANAC)
3. **Segnalanti**: Guidance sulla piattaforma per segnalazioni efficaci e anonime, Consiglio di evitare dettagli altamente personali, Informativa su conservazione dati

D) Monitoraggio e controllo

1. **Audit interno**: Revisione annuale della procedura, Revisione semestrale dei log di accesso (da dirigente diverso da RPCT), Audit annuale sulla conformità a retention policy, Audit annuale su protezione dati sensibili
2. **Incident response**: Procedura scritta per gestione violazioni dati, Notifica immediata al Titolare in caso di data breach, Valutazione entro 72 ore per segnalazione a Garante, Documentazione dell'incident
3. **Feedback segnalanti**: Raccolta periodica di feedback (entro 7 giorni dall'invio della segnalazione, entro 3 mesi, semestralmente), Valutazione se segnalanti si sentono protetti, Identificazione di problemi implementativi, Correzione della procedura se necessario
4. **Monitoraggio ritorsioni**: Raccolta di segnalazioni di discriminazione post-whistleblowing, Valutazione preliminare da parte RPCT, Escalation ad ANAC se sospetta ritorsione sistematica, Protezione temporale: garanzie specifiche per 2 anni post-segnalazione

E) Comunicazione trasparenza

1. **Informativa ai soggetti interessati** ai sensi Art. 13 GDPR
2. **Privacy notice sulla piattaforma**: esplicita nelle prime schermate
3. **FAQ per segnalanti**: risposte a domande frequenti su anonimato, conservazione, ritorsioni

6. VALUTAZIONE DELLA NECESSITÀ DI CONSULTAZIONE PREVENTIVA

Secondo l'Art. 35(4) GDPR, il Titolare del trattamento deve consultare l'Autorità Garante quando dalla DPIA emerge che il rischio non può essere efficacemente mitigato.

6.1 Criteri per consultazione (Linee Guida 35/2018 del WP29)

La consultazione è necessaria se:

1. Il trattamento comporta monitoraggio su larga scala
2. Il trattamento comporta elaborazione automatizzata con effetti giuridici
3. Il trattamento utilizza nuove tecnologie di sorveglianza
4. Il trattamento riguarda dati biometrici per identificazione
5. Il trattamento combinato di dataset ha effetti profondamente invasivi
6. Il trattamento riguarda categorie vulnerabili
7. Il trasferimento dati al di fuori UE senza adeguate garanzie

6.2 Applicazione al caso

Consultazione preventiva: NON NECESSARIA

Motivazioni:

1. **Misure tecniche robuste**: Whistleblowing Solutions ha implementato certificazioni ISO27001:2022, ISO27017:2015, ISO27018:2025, ISO9001:2015; audit annuali di sicurezza; penetration test pubblici
2. **Misure organizzative specifiche**: La presente DPIA identifica misure organizzative dettagliate che mitigano efficacemente i rischi residui
3. **Base normativa chiara**: Il D.Lgs. 24/2023 fornisce fondamento giuridico esplicito per il trattamento; le modalità sono disciplinate in modo puntuale
4. **Dati in UE**: Conservazione dati esclusivamente in Italia e UE; no trasferimenti extra-UE
5. **Monitoraggio**: Il Comune implementerà controlli periodici e procedure di audit per assicurare conformità continuativa
6. **Natura della vulnerabilità**: Il rischio principale (de-anonimizzazione in contesti piccoli) non è tecnicamente eliminabile, ma è gestibile attraverso comportamenti organizzativi (cautela nella gestione segnalazioni)
7. **Proporzionalità**: La consultazione comporterebbe ritardi significativi; il D.Lgs. 24/2023 richiede operatività rapida dei sistemi whistleblowing

Possibilità di consultazione facoltativa: Il Titolare rimane libero di sottoporre la presente DPIA all'Autorità Garante per parere facoltativo secondo l'Art. 35(9) GDPR, qualora ritenuto opportuno.

7. CONCLUSIONI E RACCOMANDAZIONI

7.1 Stato *di conformità*

La valutazione d'impatto sulla protezione dei dati per il trattamento dati relativo al sistema whistleblowing del Comune di Torri in Sabina evidenzia:

- ✓ **Necessità della DPIA**: CONFERMATA (ricorrono i criteri dell'Art. 35(1) GDPR)
- ✓ **Fondamento giuridico**: SOLIDO (Art. 6(1)(c) GDPR per obbligo legale D.Lgs. 24/2023; Art. 6(1)(e) per interesse pubblico; Art. 9(2)(h) e Art. 10 per dati sensibili)
- ✓ **Misure tecniche**: ADEGUATE (certificazioni internazionali, crittografia robusta, privacy by design, audit regolari)
- ✓ **Misure organizzative**: IMPLEMENTABILI (procedure definite, ruoli chiari, formazione prevista)
- ✓ **Rischi residui**: GESTIBILI (tutti valutati come MEDIO o BASSO con mitigazione)
- ✓ **Consultazione preventiva**: NON NECESSARIA (rischi gestibili; consultazione facoltativa rimane possibile)

PARERE SINTETICO: Il trattamento è legittimo, le misure sono proporzionate e implementabili.

Il Comune può procedere all'implementazione del sistema whistleblowing nel pieno rispetto del GDPR e del D.Lgs. 24/2023, a condizione che implementi le misure organizzative indicate nella presente DPIA.

7.2 Azioni immediate da intraprendere

1. **Approvazione della DPIA**: Delibera della Giunta comunale che approva la presente DPIA
2. **Designazione responsabili**: Decreto del Sindaco che formalizza RPCT come responsabile gestione segnalazioni e staff di supporto (se previsto)
3. **Implementazione procedura**: Adozione della "Procedura di gestione delle segnalazioni"
4. **Formazione iniziale**: Training del RPCT e staff su GDPR, D.Lgs. 24/2023, procedura, sistemi di sicurezza
5. **Informativa**: Pubblicazione della privacy notice sulla piattaforma WhistleblowingPA e sul sito internet del Comune
6. **Comunicazione interna**: Informazione a tutto il personale dell'Ente sulla disponibilità del canale whistleblowing
8. **Attivazione monitoraggio**: Installazione dei controlli di audit, log review, feedback segnalanti

7.3 Monitoraggio continuativo

La DPIA non è statica. Il Comune implementerà un piano di monitoraggio continuativo:

Frequenza	**Attività**
Semestrale	Revisione log di accesso da parte di dirigente Feedback segnalanti oltre a quelli previsti a seguito dell'invio della segnalazione (entro 7 giorni e entro 3 mesi) Audit compliance retention
Annuale	Revisione della procedura e identificazione miglioramenti Audit sulla protezione dati sensibili Valutazione complessiva DPIA Revisione formazione

In caso di cambiamenti significativi (tecnologie, volumi di segnalazioni, incident), la DPIA sarà riesaminata e aggiornata.

Il DPO

Per presa visione