COMUNE DI CASTELDELCI

(Provincia di Rimini)

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

(ART. 35 Regolamento UE 2016/679)

Informazioni sulla PIA

Nome della PIA

WHISTLEBLOWING

Nome autore

SEGRETARIA COMUNALE DOTT.SSA VALENTINA ZANGHERI

Nome valutatore

Anna Lisa Minghetti DPO- team

Nome validatore

Lepida ScpA

Mail: gdpr@lepida.it

Data di creazione

10/04/2025

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati. Il fondamento giuridico del trattamento dei dati risiede nell'assolvimento di funzioni ed obblighi di legge.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Piattaforma Whistleblowing del Comune di Casteldelci. Esso svolge funzioni di raccolta e gestione delle segnalazioni di illeciti per contrastare fenomeni corruttivi, sia nelle imprese private sia nelle pubbliche amministrazioni.

Quali sono le responsabilità connesse al trattamento?

Titolare del trattamento dei dati personali è il Comune di Casteldelci. Incarica del trattamento dei dati, secondo le scelte del titolare del trattamento dei dati, è il responsabile p.t. della prevenzione della corruzione del Comune di Casteldelci.

Responsabile (esterno) del trattamento è Whistleblowing Solutions, il gestore 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.

Seeweb riveste il ruolo di Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura (IaaS);
Transparency International Italia riveste il ruolo di Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing.

Ci sono standard applicabili al trattamento?

Utilizzo di politiche privacy indicate nel Registro del Trattamento, in particolare si applicheranno le linee guida del Garante nazionale per la protezione dei dati.
Inoltre, il servizio erogato adotta misure progettate in aderenza allo standard internazionale ISO37002:2021 in materia di gestione dei processi di whistleblowing. Il Responsabile adotta un modello di gestione integrata dei propri processi di fornitura SaaS certificato:

- **ISO/IEC 27001:2022**
- **ISO/IEC 2701:2015**
- **ISO/IEC 27018:2019**
- **ISO 9001:2015**
- **CSA STAR Level 1**
- **ACN**

Valutazione:
Commento di valutazione:

Dati, processi e risorse di supporto

Quali sono i dati trattati?

La piattaforma informatica utilizzata consente la compilazione, l'invio e la ricezione delle segnalazioni di presunti fatti illeciti nonché la possibilità per l'ufficio del Responsabile della prevenzione corruzione (RPC), che riceve tali segnalazioni, di comunicare in forma riservata con il segnalante senza conoscerne l'identità.

In particolare:

- **dati di registrazione**
- **dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (es. Responsabile Anticorruzione);**
- **inoltre, sono trattate categorie particolari di 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.**

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

Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse. La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, nonché dagli articoli 5 e seguenti del decreto legislativo 14 marzo 2013, n. 33. 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, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del decreto legislativo 24 del 2023 e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018.

Il ciclo di vita 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 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?

I dati sono gestiti mediante un'apposita piattaforma attivata dal Comune di Casteldelci tramite adesione al Portale Whistleblowing.it di Trasparency International per l'acquisizione e la gestione - nel rispetto delle garanzie di riservatezza previste dalla normativa vigente - delle segnalazioni di illeciti da parte dei dipendenti dell' Ente e per dialogare con i segnalanti anche in modo anonimo così come previsto dal Decreto Legislativo 24 del 2023 e previsto dalle Linee Guida Anac basata sul software GlobaLeaks, che permette di ricevere segnalazioni di illeciti da parte dei potenziali segnalanti e di dialogare con gli stessi, anche in modo anonimo.

Software di whistleblowing professionale GlobaLeaks. Infrastruttura IaaS e SaaS privata basata su tecnologie:
- Dettaglio Hardware
- VMWARE (virtualizzazione)
- Debian Linux LTS (sistema operativo)

- VEEAM (backup)
- OPNSENSE (firewall)
- OPENVPN (vpn)

Valutazione:
Commento di valutazione:

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento in questione comporta il conferimento al Responsabile della Prevenzione della Corruzione (RPC) dell'ente, tramite compilazione di un form su apposita piattaforma whistleblowingPA , di dati anagrafici, codice fiscale, dati di contatto e, eventualmente, dati sulla qualifica professionale, nonché di dati e informazioni ulteriori connessi alla condotta illecita riportata.
I dati forniti verranno trattati esclusivamente per l'istruttoria della segnalazione ai sensi del Decreto Legislativo 24 del 10 marzo 2023.
Al fine di garantire la riservatezza del segnalante per tutta la durata della gestione della segnalazione, l'identità dello stesso sarà conosciuta solo dal Responsabile della Prevenzione della Corruzione (RPC) dell'ente e dai fornitori del servizio della piattaforma whistleblowingPA. Ad eccezione dei casi in cui sia configurabile una responsabilità a titolo di calunnia e di diffamazione ai sensi delle disposizioni del codice penale o dell'art. 2043 del codice civile e delle ipotesi in cui l'anonimato non sia opponibile per legge (ad esempio, indagini penali, tributarie o amministrative, ispezioni di organi di controllo), l'identità del segnalante viene protetta in ogni contesto successivo alla segnalazione. Pertanto, fatte salve le citate eccezioni, l'identità del segnalante non può essere rivelata senza il suo espresso consenso, e tutti coloro che ricevono o sono coinvolti nella gestione della segnalazione sono tenuti a tutelare la riservatezza di tale informazione. In questo ambito, i trattamenti di dati personali effettuati dai soggetti obbligati possono essere considerati necessari per adempiere a un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, § 1, lett. c) del Regolamento), e, con riguardo a categorie particolari di dati (art. 9, § 2, lett. b) del Regolamento in relazione all'art. 54-bis,) o a dati relativi a condanne penali e reati, possono, altresì, essere considerati necessari per l'esecuzione di un compito di interesse pubblico contemplato dall'ordinamento (art. 6, § 1, lett. e) e art. 9, § 2, lett. g) e 10 del Regolamento). Il trattamento dei dati personali è improntato ai principi di correttezza, liceità e trasparenza e di tutela della riservatezza e dei diritti dell'interessato, nonché agli ulteriori principi previsti dall'art. 5 del Regolamento. Tali attività sono esplicitate attraverso specifica informativa ai sensi dell'articolo 13 del Regolamento Ue 679/2016 messa a disposizione sul sito web del Comune di Casteldelci, nella pagina dedicata al canale whistleblowing.

Valutazione:
Commento di valutazione:

Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento si basa sulle competenze attribuite dalla legge all'ente e, tra le altre, in particolare dal d.lgs.267/2000 "Testo Unico degli Enti Locali", dalla Legge 30 Novembre 2017, n. 179 "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato.", dalla Legge 6 Novembre 2012, n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e della illegalità nella pubblica amministrazione.", dal Decreto Legislativo 10 marzo 2023, n. 24 "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali."

Valutazione:

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 sono richiesti unicamente i seguenti dati:
Nome, Cognome, Ruolo, Telefono, Email di ruolo dell'utente che effettua la registrazione 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.

Il trattamento dei dati personali verrà effettuato esclusivamente dal Responsabile della Prevenzione della Corruzione (RPC) dell'ente e dai fornitori della piattaforma di whistleblowing con l'utilizzo di procedure anche informatizzate, dotate di strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e del contenuto delle segnalazioni e della relativa documentazione, adottando misure tecniche e organizzative adeguate a proteggerli da accessi non autorizzati o illeciti, dalla distruzione, dalla perdita d'integrità e riservatezza, anche accidentali.
I dati verranno conservati per 12 mesi e comunque per tutta la durata dell'eventuale procedimento disciplinare, penale o dinanzi la Corte dei Conti. I dati personali non saranno comunicati ad altri soggetti, ad esclusione dei casi sopra indicati, così come non saranno oggetto di diffusione.

Valutazione:

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.

Valutazione: :

Qual è il periodo di conservazione dei dati?

Ai sensi dell'articolo 14 del D.Lgs. 24 del 10 marzo 2023 le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre 12 mesi a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del decreto legislativo citato e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018.

Valutazione:

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Ai sensi dell'articolo 13 del D.Lgs. 24 del 10 marzo 2023, ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti viene effettuato a norma del regolamento (UE) 2016/679, del decreto legislativo 30 giugno 2003, n. 196 e del decreto legislativo 18 maggio 2018, n. 51.
I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente. Sono fornite idonee informazioni alle persone segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14 del medesimo regolamento (UE) 2016/679 o dell'articolo 11 del citato decreto legislativo n. 51 del 2018 con informativa specifica messa a disposizione sul sito web del Comune di Casteldelci, alla pagina dedicata al canale.

Valutazione:

Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso degli interessati non è richiesto in quanto il fondamento giuridico del trattamento risiede nell'assolvimento di funzioni ed obblighi di legge.

Valutazione:

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

Gli interessati del trattamento hanno diritto di ottenere dall'ente la rettifica, l'integrazione, la cancellazione degli stessi o la limitazione del trattamento ovvero di opporsi al trattamento medesimo (artt. 15 e ss. del Regolamento). L'interessato potrà esercitare tutti i diritti di cui sopra inviando una e-mail al Responsabile della prevenzione della corruzione (RPC) all'indirizzo di posta elettronica personale disponibile alla home page dell'ente o inviando una pec all'indirizzo: protocollo.comune.casteldelci@pec.it. Gli interessati che ritengano che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dal Regolamento hanno, inoltre, il diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali, come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).
Nella informativa presente sulla home page istituzionale dell'Ente è indicato il riferimento del titolare del trattamento, del DPO/RDP e del Garante Italiano per la protezione dei dati personali, con gli indirizzi mail e fisici, ai quali rivolgersi per avere informazioni ovvero per segnalare eventuali violazioni.

Valutazione:

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

Il diritto all'oblio si realizza automaticamente entro i termini previsti dalla norma per cui i dati sono conservati per 12 mesi e comunque per tutta la durata dell'eventuale procedimento disciplinare.

Valutazione:

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

L'interessato potrà esercitare i diritti di limitazione ed opposizione inviando una e-mail al Responsabile della prevenzione della corruzione (RPC) all'indirizzo di posta elettronica personale disponibile alla home page dell'ente o inviando una pec all'indirizzo: protocollo.comune.casteldelci@pec.it .
Nella informativa presente sulla home page istituzionale dell'Ente è indicato il riferimento del titolare del trattamento, del DPO/RDP, del RPC, del Garante Italiano per la protezione dei dati personali, con gli indirizzi mail e fisici, ai quali rivolgersi per avere informazioni ovvero per segnalare eventuali violazioni.

Valutazione:

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

Sono contenuti nel documento "WBIT - documentazione supporto dpia" relativo all'adesione alla piattaforma whistleblowingPA.

Valutazione:

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

Non è previsto alcun trasferimento al di fuori dell'Unione Europea.

Valutazione:

Rischi

Misure esistenti o pianificate

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.

Protocollo crittografico: https://docs.globaleaks.org/en/stable/security/EncryptionProtocol.html

Valutazione:

Sicurezza dei documenti cartacei

I documenti cartacei vengono conservati dal responsabile per la prevenzione della corruzione e della trasparenza che verifica che siano disposti in specifici raccoglitori in modo tale che non vadano dispersi e che non siano visibili a terzi non autorizzati, gli uffici devono essere chiusi e l'accesso consentito soltanto agli addetti o i soggetti autorizzati.

Valutazione:

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. Ogni log di audit viene mantenuto per un periodo massimo di 5 anni, fatto salvo il caso specifico dei log pertinenti le segnalazioni che vengono mantenuti per tutto il tempo di conservazione delle stesse.
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.

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

BACKUP

I sistemi sono soggetti a backup remoto con frequenza di 8 ore e policy di data retention di 7 giorni necessari per finalità di disaster recovery garantendo dunque una RPO di 8 ore.

MANUTENZIONE

E' 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.

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare*?*

Qualora fosse realizzato un accesso abusivo al sistema da soggetti attrezzati e travisati e fosse possibile asportare la memoria di massa senza il pronto intervento dei sistemi di sicurezza, i dati sarebbero crittografati, quindi si tratterebbe di un impatto limitato.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Furto, Vandalismo.

Quali sono le fonti di rischio?

Interne, esterne, non umane.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Specifiche Misure di Sicurezza fornite dal gestore della piattaforma.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitato, poiché il sistema di crittografia e il posizionamento del computer di accesso in un locale sicuro e presidiato qual è l'ufficio del responsabile per la prevenzione della corruzione e della trasparenza rendono molto limitato il rischio di accesso abusivo ai dati e limitato il rischio di distruzione degli stessi.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, sulla base delle misure pianificate.

Valutazione:

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Qualora fosse realizzato un accesso abusivo al sistema da soggetti attrezzati e travisati e fosse possibile asportare la memoria di massa senza il pronto intervento dei sistemi di sicurezza, i dati sarebbero crittografati, quindi si tratterebbe di un impatto limitato.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Errore materiale, evento doloso o abuso/violazione da parte degli addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzati.

Quali sono le fonti di rischio?
Esterne, interne, non umane.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Specifiche Misure di Sicurezza, Sicurezza dei documenti cartacei.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?
Limitata, il sistema di crittografia e il controllo logico degli accessi rende pressoché impossibile l'accesso ai dati ai fini della modifica se non ai soggetti autorizzati e quindi formati e competenti.

Valutazione:

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?
Perdita delle informazioni.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?
Errore materiale, furto, vandalismo, danno o malfunzionamento del sistema di registrazione dei dati.

Quali sono le fonti di rischio?
Esterne, interne, non umane.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Specifiche Misure di Sicurezza, Sicurezza dei documenti cartacei.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Limitata, in quanto il server che ospita il servizio è collocato in ambiente cloud in grado di garantire un elevato livello di resilienza ai guasti e ai disservizi nonché da un giornaliero backup delle informazioni.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Limitata, i sistemi di sicurezza adottati rendono trascurabile il rischio.

Valutazione:

Piano d'azione

Panoramica

Principi fondamentali	Misure esistenti o pianificate
Finalità	
Basi legali Adeguatezza dei dati	Copia di backup dei dati
Esattezza dei dati	Blocco all'installazione di sw dannosi
Periodo di conservazione	
Informativa	
	Crittografia
	Antimalware
Diritto di rettifica e diritto di cancellazione	Nomina di sostituti temporanei
Diritto di limitazione e diritto di opposizione	Crittografia
Responsabili del trattamento	
Trasferimenti di dati	

Rischi

Accesso illegittimo ai dati

Modifiche indesiderate dei dati

Perdita di dati

Misure Migliorabili

Misure Accettabili

Principi fondamentali

La DPIA ha accertato la conformità del trattamento. Nessuna azione correttiva necessaria.

Misure esistenti o pianificate

Le misure di sicurezza esistenti risultano adeguate. Non si prevedono ulteriori implementazioni al momento.

Rischi

I rischi identificati (accesso non autorizzato, modifica indesiderata, perdita dati) risultano mitigati in modo efficace. Nessuna azione aggiuntiva è attualmente necessaria.

Conclusioni

In esito all'analisi condotta, si ritiene che il trattamento dei dati personali connesso alla gestione del canale di whistleblowing attivato dal Comune di Casteldelci sia conforme ai principi sanciti dal Regolamento (UE) 2016/679, con particolare riferimento agli articoli 5, 6, 9 e 32, nonché alle disposizioni del D.lgs. 24/2023. Il sistema implementato garantisce elevati standard di sicurezza, in particolare grazie all'utilizzo della piattaforma GlobaLeaks, progettata secondo criteri di privacy by design e by default, nonché al ricorso a tecniche di crittografia avanzata, audit log riservati e misure di backup periodico.

La valutazione ha rilevato che:

- il trattamento rispetta i principi di liceità, correttezza, trasparenza, minimizzazione e limitazione della conservazione;
- i rischi per i diritti e le libertà degli interessati risultano **limitati**, grazie all'efficacia delle misure tecniche e organizzative adottate;
- non si evidenziano necessità di ulteriori interventi correttivi né azioni integrative al momento.

Il livello di rischio è basso, tuttavia si raccomanda comunque un **monitoraggio periodico** della piattaforma, con verifica almeno annuale dell'adeguatezza delle misure di sicurezza adottate e aggiornamento della DPIA in caso di modifiche significative del trattamento o dei fornitori coinvolti.