



## DPIA

### Informazioni sulla PIA

---

Nome della PIA: SEGNALAZIONI DI VIOLAZIONI DELLE DISPOSIZIONI NORMATIVE AI SENSI DEL DECRETO LEGISLATIVO 10 MARZO 2023, n. 24 (WHISTLEBLOWING)

Nome autore: il Responsabile della Prevenzione della Corruzione e della Trasparenza

Data di creazione: 10 settembre 2024

Nome del DPO/RPD: avvocato Vicenzotto Paolo

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non si ritiene opportuno procedere alla richiesta di alcun parere agli Interessati.

### Contesto

---

#### Panoramica del trattamento

##### Quale è il trattamento in considerazione?

Il trattamento oggetto di valutazione con la presente DPIA riguarda la gestione della raccolta delle segnalazioni whistleblowing attraverso i seguenti canali di segnalazione:

- effettuata mediante la piattaforma disponibile al link <https://amministrazionetrasparente.provincia.treviso.it/index.php/altri-contenuti/category/514-segnalazioni-di-illecito> ;
- su richiesta della persona segnalante, mediante un incontro diretto con il RPCT. Ai sensi di quanto previsto dall'articolo 14, comma 4, del decreto legislativo 10 marzo 2023, n. 24, previo consenso della persona segnalante, la segnalazione è documentata mediante verbale che il segnalante conferma mediante la propria sottoscrizione. La segnalazione ricevuta vedrà separati i dati identificativi del segnalante dalla segnalazione per tutta la durata dell'istruttoria del procedimento, rendendo impossibile risalire all'identità del segnalante se non nei casi in cui l'anonimato non è opponibile per legge. Tutti i documenti cartacei saranno custoditi e conservati in apposito armadio chiuso a chiave situato presso l'ufficio del Responsabile della Prevenzione della Corruzione e Trasparenza e accessibile solo alle persone appositamente dallo stesso autorizzate.

##### Quali sono le responsabilità connesse al trattamento?

Le segnalazioni eseguite nell'ambito degli incontri diretti con il RPCT vengono trattate esclusivamente dal RPCT. Se si utilizza la piattaforma web sono coinvolti, per esclusive ragioni tecniche e di manutenzione, anche:

- **Whistleblowing Solutions** > Responsabile del trattamento per la fornitura e la gestione del sistema di whistleblowing



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

### Ci sono standard applicabili al trattamento?

Alle segnalazioni tramite piattaforma web sono applicati i seguenti standard:

- 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

### Dati, processi e risorse di supporto

#### Quali sono i dati trattati?

I dati personali raccolti e trattati nell'ambito della segnalazione possono includere dati personali "comuni" del "Segnalante", del "Segnalato" e delle persone coinvolte e/o collegate ai fatti oggetto della segnalazione (ad es. dati anagrafici, funzioni, recapiti quali: indirizzo mail, indirizzo postale, numero telefonico, dati sulla qualifica professionale ricoperta, dati e informazioni ulteriori connessi alla condotta illecita). E' possibile che, in alcuni casi, ove necessario, siano altresì trattati dati appartenenti a particolari categorie ex art. 9 e/o 10 del GDPR.

#### Qual è il ciclo di vita del trattamento dei dati?

Le segnalazioni presentate e la relativa documentazione saranno 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.

#### Quali sono le risorse di supporto ai dati?

Le informazioni di seguito riportate si riferiscono alle segnalazioni tramite piattaforma web.

### 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 e 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 diverse componenti secondo la 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.

### Principi Fondamentali

---

#### Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Lo scopo del trattamento è permettere di segnalare condotte illecite all'interno dell'Ente. Si precisa che, per poter godere delle tutele previste dall'art. 3 della L. n. 179/2017, gli illeciti devono essere conosciuti in virtù del rapporto di lavoro ovvero in occasione dello svolgimento del rapporto di servizio o fornitura o realizzazione di opera in favore dell'Ente.

Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento è lecito ai sensi dell'art. 6 par. 1 lett. C ed E del GDPR. Alcuni trattamenti specifici si basano inoltre sul consenso del segnalante.

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

Il segnalante è tenuto a fornire tutti gli elementi utili a consentire agli uffici competenti di procedere alle dovute e appropriate verifiche a riscontro della fondatezza dei fatti oggetto di



segnalazione. A tal fine, la segnalazione deve preferibilmente contenere i seguenti elementi:

- a) generalità del soggetto che effettua la segnalazione con indicazione della posizione o funzione svolta nell'ambito dell'Ente;
- b) la chiara e completa descrizione dei fatti oggetto di segnalazione;
- c) se conosciute, le circostanze di tempo e di luogo in cui sono stati commessi;
- d) se conosciute, le generalità o altri elementi (come la qualifica e il servizio in cui svolge l'attività) che consentano di identificare il soggetto che ha posto in essere i fatti oggetto di segnalazione;
- e) l'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;
- f) l'indicazione di eventuali documenti che possono confermare la fondatezza di tali fatti;
- g) ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

**I dati sono esatti e aggiornati?**

Non applicabile al trattamento in oggetto.

**Qual è il periodo di conservazione dei dati?**

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.

**Misure a tutela dei diritti degli interessati**

**Come sono informati del trattamento gli interessati?**

Gli interessati sono informati attraverso l'informativa privacy specifica messa a disposizione in fase di presentazione della segnalazione e attraverso la procedura per poter effettuare la segnalazione. Entrambi i documenti sono pubblicati all'interno del sito web istituzionale.

**Gli interessati sono messi in grado di esercitare i diritti di cui agli artt. 15 e seguenti?**

Sì, con le modalità indicate nell'informativa del punto precedente.

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

Gli accordi contrattuali sono 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

**I dati sono trasferiti al di fuori del territorio UE?**

No.

**Rischi**

---

**Indisponibilità dei dati (distruzione, perdita, furto)**

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



- sicurezza e l'incolumità del segnalante;
- ritorsioni;
- emarginazione sociale nell'ambiente lavorativo;
- danno reputazionale.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

- Accesso fisico al PC del RPPCT;
- Virus informatici;
- Errore umano.

Quali sono le fonti di rischio?

- Ambiente fisico non protetto;
- Rete internet;
- Errore umano.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

- Password;
- installazione antivirus;
- apertura file e stampa documenti relativi in stanza chiusa (no stampanti di rete);
- formazione;
- disaccoppiamento dei dati relativi al segnalante rispetto alla segnalazione e alla relativa documentazione.

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

**Medio**

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

**Improbabile.**

**Integrità dei dati (alterazione, modifica)**

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

- sicurezza e l'incolumità del segnalante;
- ritorsioni;
- emarginazione sociale nell'ambiente lavorativo;
- danno reputazionale.

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

Accesso fisico al PC del RPPCT;

- Virus informatici;
- errore umano.

Quali sono le fonti di rischio?

- Ambiente fisico non protetto;



- rete internet;
- errore umano.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

- Password;
- installazione antivirus;
- apertura file e stampa documenti relativi in stanza chiusa (no stampanti di rete);
- formazione;
- disaccoppiamento dei dati relativi al segnalante rispetto alla segnalazione e alla relativa documentazione.

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

**Medio**

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

**Improbabile.**

**Riservatezza dei dati (accesso abusivo, trattamento non conforme)**

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

- sicurezza e l'incolumità del segnalante;
- ritorsioni;
- emarginazione sociale nell'ambiente lavorativo;
- danno reputazionale.

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

- Accesso fisico al PC del RPPCT;
- virus informatici;
- errore umano.

Quali sono le fonti di rischio?

- Ambiente fisico non protetto;
- rete internet;
- errore umano.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

- Password;
- installazione antivirus;
- apertura file e stampa documenti relativi in stanza chiusa (no stampanti di rete);
- formazione;
- disaccoppiamento dei dati relativi al segnalante rispetto alla segnalazione e alla relativa documentazione.



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

**Medio**

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

**Improbabile.**

## Piano d'azione

### Misure e Procedure adottate o programmate per la mitigazione dei rischi

Le informazioni di seguito riportate si riferiscono alle segnalazioni tramite piattaforma web.

#### **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 SSLabs 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 applicativo è consentito a ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.

Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password.

Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238.

Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

#### **TRACCIABILITÀ**

L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing.

I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent.

I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.

#### **ARCHIVIAZIONE**

L'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM. 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 GlobalLeaks 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**

E' prevista manutenzione periodica correttiva, evolutiva e con finalità di migioria 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.

## **Parere del DPO/RPD**

A seguito dell'analisi del documento, visto l'art. 39 par. 1 lett. C del Reg. 679/2016, il DPO ritiene che i rischi per i diritti e le libertà degli interessati, a seguito dell'adozione delle misure di mitigazione del rischio indicato, possano essere qualificati come rischi accettabili in relazione alle finalità perseguite dal trattamento in oggetto. Nello specifico non si ritiene esistente un "rischio elevato" come inteso dall'art. 35 GDPR; per tale ragione, inoltre, non si rende necessario procedere con la consultazione preventiva ex art. 36 GDPR.

L'autore

il Responsabile della Prevenzione della Corruzione e della  
Trasparenza della Provincia di Treviso, Bassani Manuela

Il Validatore / DPO

avvocato Vicenzotto Paolo in nome del Centro Studi Amministrativi  
della Marca Trevigiana  
(firmato digitalmente ai sensi D.lgs 82/2005)