WHISTLEBLOWING

TO TRANSLATE - Editing :
Rosa Santaniello
TO TRANSLATE - Evaluation :
Pierantonio Massafra
TO TRANSLATE - Validation :
Pierantonio Massafra
TO TRANSLATE - Status :
Validata
100%

TO TRANSLATE - Validation

Mappaggio dei rischi

TO TRANSLATE - Validation

Piano d'azione

Principi fondamentali

Nessun piano d'azione registrato.

Misure esistenti o pianificate

Nessun piano d'azione registrato.

Rischi

Nessun piano d'azione registrato.

TO TRANSLATE - Validation

TO TRANSLATE - DPO and data subjects opinion

Nome del DPO/RPD

Ing. Massafra Pierantonio

Posizione del DPO/RPD

Il trattamento puÃ² essere implementato.

Parere del DPO/RPD

A seguito di attenta analisi del presente documento, visto lâ€™art. 39 par. 1 lett. C) del Reg.UE 2016/679, tenuto conto: - dellâ€™adozione da parte del Titolare del trattamento di politiche di controllo periodiche in riferimento ai dati oggetto del trattamento in questione e alle misure esistenti o pianificate (misure applicate ai dati, misure generali di sicurezza dei sistemi e misure organizzative); - della esecuzione di una precisa e rigorosa manutenzione dei sistemi; - della costante formazione del personale designato/autorizzato al trattamento dei dati, ritiene che i rischi per i diritti e le libertÃ fondamentali degli interessati, relativi ai trattamenti in discorso, possano essere qualificati come medio-bassi. Pertanto, nel complesso, alla data odierna, non si ritiene esistente un â€œrischio elevatoâ€ come inteso dallâ€™art. 35 Reg. UE 2016/679. Per tale ragione, non si ritiene necessario procedere con la Consultazione preventiva ex art. 36 Reg. UE 2016/679

Richiesta del parere degli interessati

Non Ã¨ stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non eÌ€ stato ritenuto necessario, anche in considerazione degli esiti della presente valutazione, acquisire il parere dei potenziali interessati.

Contesto

Panoramica del trattamento

Quale Ã¨ il trattamento in considerazione?

Le operazioni di trattamento dati che l'Unione dei Comuni Lombarda della Valletta per il sistema di segnalazione sicura, che protegga la riservatezza dellâ€™identitÃ e i dati personali di chi denuncia condotte illecite. L'obbligo di implemenzazione del portale di whistleblowing Ã¨ contenute nel Dlgs 24/2023. Con questo decreto il legislatore, in attuazione di alcuni principi comunitari espressi nella direttiva Ue 2019/1937

Quali sono le responsabilitÃ connesse al trattamento?

PA, Ente o Organizzazione > Titolare del trattamento

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 dellâ€™infrastruttura (IaaS)

Transaparency 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?

La soluzione scelta ha le seguenti certificazioni:
â— ISO27001 â€œErogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaksâ€ â— ISO27017 controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud â— ISO27018 per la protezione dei dati personali nei servizi Public Cloud â— Qualifica AGID â— Certificazione CSA Star

Valutazione : Accettabile
Commento di valutazione :
ok

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per lâ€™erogazione dei servizi in modalitÃ SaaS cosÃ¬ come pattuito tra le parti. Dati di registrazione Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (es. Responsabile Anticorruzione). 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.

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

1) Attivazione della piattaforma
2) Configurazione della piattaforma
3) Fase dâ€™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 finalitÃ amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore

Quali sono le risorse di supporto ai dati?

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 : Accettabile
Commento di valutazione :
dati forniti dal fornitore del servizio

Principi Fondamentali

ProporzionalitÃ e necessitÃ

Gli scopi del trattamento sono specifici, espliciti e legittimi?

il sistema permette: segnalazione sicura, che protegga la riservatezza dellâ€™identitÃ e i dati personali di chi denuncia condotte illecite come indicato nel Dlgs 24/2023

Valutazione : Accettabile
Commento di valutazione :
ok

Quali sono le basi legali che rendono lecito il trattamento?

Sulla base di quanto sopra indicato la liceitÃ del trattamento Ã¨ individuabile del whistleblowing sono contenute nel Dlgs 24/2023. Con questo decreto il legislatore, in attuazione di alcuni principi comunitari espressi nella direttiva Ue 2019/1937

Valutazione : Accettabile
Commento di valutazione :
come da normativa vigente

I dati raccolti sono adeguati, pertinenti e limitati a quanto Ã¨ necessario in relazione alle finalitÃ 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 dellâ€™utente che effettua la registrazione e i dati relativi allâ€™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 dellâ€™anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata.
Lâ€™applicativo GlobaLeaks vede abilitata la possibilitÃ di navigazione tramite Tor Browser per finalitÃ accesso anonimo con garanzie al passo con lo stato dellâ€™arte della ricerca tecnologica in materia.

Valutazione : Accettabile
Commento di valutazione :
ok

I dati sono esatti e aggiornati?

Lâ€™aggiornamento dei dati Ã¨ a cura degli utenti stessi che si sono registrati attraverso lâ€™accesso alla propria area riservata.
Non appena vengono modificati i dati di contatto allâ€™interno della piattaforma, questi diventano i dati di contatto ufficiali a

cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.

Valutazione : Accettabile
Commento di valutazione :
ok

Qual Ã¨ il periodo di conservazione dei dati?

Policy di data retention di default delle segnalazioni di 18 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute.
Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio.

Valutazione : Accettabile
Commento di valutazione :
ok

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Si specifica che nella sezione â€œprivacyâ€□ del sito web istituzionale dell'Unine dei Comuni lombarda della Valletta viene riportata lâ€™informativa completa sul trattamento dei dati de sistema di whistleblowing ai sensi dellâ€™art. 13 del reg. 679/16.

Valutazione : Accettabile
Commento di valutazione :
ok

Ove applicabile: come si ottiene il consenso degli interessati?

In relazione al trattamento dei dati personali, Ã¨ assicurato agli interessati, identificati o identificabili, l'effettivo esercizio dei propri diritti, in particolare quello di accedere ai dati che li riguardano, di verificarne le finalitÃ , le modalitÃ del trattamento e di ottenerne lâ€™interruzione nel caso di utilizzo illecito.

Valutazione : Accettabile
Commento di valutazione :
ok

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

In relazione al trattamento dei dati personali, Ã¨ assicurato agli interessati, identificati o identificabili, l'effettivo esercizio dei propri diritti, in particolare quello di accedere ai dati che li riguardano, di verificarne le finalitÃ , le modalitÃ del trattamento e di ottenerne lâ€™interruzione nel caso di utilizzo illecito.

Valutazione : Accettabile
Commento di valutazione :
ok

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

In relazione al trattamento dei dati personali, Ã¨ assicurato agli interessati, identificati o identificabili, l'effettivo esercizio dei propri diritti, in particolare quello di accedere ai dati che li riguardano, di verificarne le finalitÃ , le modalitÃ del trattamento e di ottenerne lâ€™interruzione nel caso di utilizzo illecito.

Valutazione : Accettabile
Commento di valutazione :
ok

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

In relazione al trattamento dei dati personali, Ã¨ assicurato agli interessati, identificati o identificabili, l'effettivo esercizio dei propri diritti, in particolare quello di accedere ai dati che li riguardano, di verificarne le finalitÃ , le modalitÃ del trattamento e di ottenerne lâ€™interruzione nel caso di utilizzo illecito.

Valutazione : Accettabile
Commento di valutazione :
ok

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

Gli accordi contrattuali sono definiti con le seguenti societÃ :

- Whistleblowing Solutions in qualitÃ di Responsabile del trattamento
- Seeweb in qualitÃ di Sub-Responsabile del trattamento nominato da Whistleblowing Solutions

- Transparency International Italia in qualitÃ di Sub-Responsabile del trattamento nominata da Whistleblowing Solutions

Valutazione : Accettabile
Commento di valutazione :
ok

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

I Dati Personali sono trattati principalmente in Italia ed
esclusivamente nei Paesi dellâ€™Unione Europea.
Non esiste alcun trasferimento di Dati Personali verso lâ€™estero
in paesi extra UE.

Valutazione : Accettabile
Commento di valutazione :
ok

Rischi

Misure esistenti o pianificate

Crittografia

Lâ€™applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per
applicazioni di whistleblowing in collaborazione con lâ€™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 Ã¨ installato su sistema operativo Linux su cui Ã¨ 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

Valutazione : Accettabile
Commento di valutazione :
ok, misura implementata dal fornitore del servizio

Controllo degli accessi logici

Lâ€™accesso applicativo Ã¨ 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.

Valutazione : Accettabile
Commento di valutazione :
ok, misura implementata dal fornitore del servizio

TracciabilitÃ

Lâ€™applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attivitÃ effettuate dagli utenti e dal sistema in compatibilitÃ con la massima confidenzialitÃ richiesta dal processo di whistleblowing.
I log delle attivitÃ 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.

Valutazione : Accettabile
Commento di valutazione :
ok, misura implementata dal fornitore del servizio

Archiviazione

Lâ€™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 dellâ€™applicativo delle funzionalitÃ sicurezza del database e delle policy di data retention e cancellazione sicura.

Valutazione : Accettabile
Commento di valutazione :
ok, misura implementata dal fornitore del servizio

VulnerabilitÃ

Lâ€™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 finalitÃ di peer review.
A questi si aggiunge la peer review indipendente realizzata dalla crescente comunitÃ di stakeholder composta da un crescente numero di societÃ 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

Valutazione : Accettabile
Commento di valutazione :
ok, misura implementata dal fornitore del servizio

Backup

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

Valutazione : Accettabile
Commento di valutazione :
ok, misura implementata dal fornitore del servizio

Manutenzione

E' prevista manutenzione periodica correttiva, evolutiva e con finalitÃ di miglioria continua in materia di sicurezza.
Per i server applicativi virtuali che realizzano il servizio di whistleblowing Ã¨ prevista una modalitÃ di manutenzione accessibile al solo personale Whistleblowing Solutions attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.
Per i sistemi che compongono lâ€™infrastruttura fisica, di backup e firewall Ã¨ prevista una modalitÃ di manutenzione accessibile al solo personale Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

Valutazione : Accettabile
Commento di valutazione :
ok, misura implementata dal fornitore del servizio

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.

Valutazione : Accettabile
Commento di valutazione :
ok, misura implementata dal fornitore del servizio

Sicurezza dell'hardware

I datacenter del fornitore IaaS dispongono di unâ€™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.

Valutazione : Accettabile
Commento di valutazione :
ok, misura implementata dal fornitore del servizio

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.

Valutazione : Accettabile
Commento di valutazione :
ok, misura implementata dal fornitore del servizio

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 dellâ€™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.

Valutazione : Accettabile
Commento di valutazione :
ok, misura implementata dal fornitore del servizio

Rischi

Accesso illegittimo ai dati

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

Qualora il rischio si dovesse concretizzare gli interessati potrebbero sperimentare IMPATTI LIMITATI, ovvero, inconvenienti significativi, superabili nonostante alcune difficoltaÌ€

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Le minacce principali che potrebbero concretizzare il rischio sono le seguenti: Attacco Hacker attraverso la rete internet; Attacco Hacker attraverso la rete dati interna; Attacco Hacker attraverso la posta elettronica; Attacco Hacker attraverso Virus o Malware.

Quali sono le fonti di rischio?

Le fonti di rischio potrebbero essere rappresentate da una persona, interna o esterna allâ€™Ente, operante in via accidentale o intenzionale (es.: amministratore IT, utente, attaccante esterno, concorrente), o fonte non umana (acqua, materiali pericolosi, virus informatici generici) che puoÌ€ essere allâ€™origine di un rischio. Le motivazioni potrebbero essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, allâ€™acquisizione di dati per fini di ulteriore sfruttamento.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, TracciabilitÃ , Lotta contro il malware, Crittografia, VulnerabilitÃ , Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Archiviazione, Manutenzione, Sicurezza dei canali informatici, Sicurezza dell'hardware, Backup

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

Limitata, La gravitaÌ€ del rischio stimata eÌ€: LIMITATA

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

Trascurabile, La probabilitaÌ€ del rischio stimata eÌ€: TRASCURABILE

Valutazione : Accettabile
Commento di valutazione :

Tutte le misure tecniche e organizzative messe in atto adottate dal Titolare del trattamento, sopra specificate, contribuiscono a mitigare il rischio.

Rischi

Modifiche indesiderate dei dati

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

Qualora il rischio si dovesse concretizzare gli interessati potrebbero sperimentare IMPATTI LIMITATI, ovvero, inconvenienti signi+icativi, superabili nonostante alcune difficoltaÌ€.

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

Come giaÌ€ detto precedentemente le minacce principali sono le seguenti: Attacco Hacker attraverso la rete internet; Attacco Hacker attraverso la rete dati interna; Attacco Hacker attraverso la posta elettronica; Attacco Hacker attraverso Virus o Malware.

Quali sono le fonti di rischio?

Le fonti di rischio potrebbero essere rappresentate da una persona, interna o esterna allâ€™Ente, operante in via accidentale o intenzionale (es.: amministratore IT, utente, attaccante esterno, concorrente), o fonte non umana (acqua, materiali pericolosi, virus informatici generici) che puoÌ€ essere allâ€™origine di un rischio. Le motivazioni potrebbero essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, allâ€™acquisizione di dati per fini di ulteriore sfruttamento.

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

Controllo degli accessi logici, TracciabilitÃ , Archiviazione, Sicurezza dei canali informatici, Sicurezza dell'hardware, Manutenzione, Lotta contro il malware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Crittografia, Backup

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

Limitata, La gravitaÌ€ del rischio stimata eÌ€: LIMITATA.

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

Trascurabile, La gravitaÌ€ del rischio stimata eÌ€: TRASCURABILE.

Valutazione : Accettabile
Commento di valutazione :
Tutte le misure tecniche e organizzative messe in atto adottate dal Titolare del trattamento, sopra specificate, contribuiscono a mitigare il rischio.

Rischi

Perdita di dati

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

Qualora il rischio si dovesse concretizzare gli interessati potrebbero sperimentare un IMPATTO LIMITATO, ovvero, inconvenienti signi+icativi, superabili nonostante alcune dif+icoltaÌ€. In caso di accesso illegittimo alle immagini si ritiene non si concretizzi un danno rilevante, in quanto il soggetto prenderebbe semplicemente visione.

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

Come giaÌ€ detto precedentemente le minacce principali sono le seguenti: Attacco Hacker attraverso la rete internet; Attacco Hacker attraverso la rete dati interna; Attacco Hacker attraverso la posta elettronica; Attacco Hacker attraverso Virus o Malware.

Quali sono le fonti di rischio?

Le fonti di rischio potrebbero essere rappresentate da una persona, interna o esterna allâ€™Ente, operante in via accidentale o intenzionale (es.: amministratore IT, utente, attaccante esterno, concorrente), o fonte non umana (acqua, materiali pericolosi, virus informatici generici) che puoÌ€ essere allâ€™origine di un rischio. Le motivazioni potrebbero essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, allâ€™acquisizione di dati per fini di ulteriore sfruttamento.

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

Crittografia, Controllo degli accessi logici, TracciabilitÃ , Archiviazione, Backup, Manutenzione, Sicurezza dei canali informatici, Sicurezza dell'hardware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Lotta contro il malware

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

Limitata, La gravitaÌ€ del rischio stimata eÌ€: LIMITATA

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

Trascurabile, La probabilitaÌ€ del rischio stimata eÌ€: TRASCURABILE

Valutazione : Accettabile
Commento di valutazione :
Tutte le misure tecniche e organizzative messe in atto adottate dal Titolare del trattamento, sopra specificate, contribuiscono a mitigare il rischio.

Rischi

Panoramica dei rischi