# TO TRANSLATE - Preview

## TO TRANSLATE - GENERAL INFORMATION

modifica pia

*100%*

Anteprima

| | | | |
|---|---|---|---|
| **TO TRANSLATE - Editing :** | SARA SCIPIONI | **TO TRANSLATE - Status :** | Validata |
| **TO TRANSLATE - Evaluation :** | DIRETTORE GENERALE STEFANO BECCARINI | | |
| **TO TRANSLATE - Validation :** | DPO GIACOMO MARCHIONI | | |

# TO TRANSLATE - Validation

## Mappaggio dei rischi

### Gravità del rischio


### Probabilità del rischio

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

11/05/23

# TO TRANSLATE - Validation

## Piano d'azione

## Panoramica

### Principi fondamentali

Finalità
Basi legali
Adeguatezza dei dati
Esattezza dei dati
Periodo di conservazione
Informativa
Raccolta del consenso
Diritto di accesso e diritto alla portabilità dei dati
Diritto di rettifica e diritto di cancellazione
Diritto di limitazione e diritto di opposizione
Responsabili del trattamento
Trasferimenti di dati

### Misure esistenti o pianificate

Crittografia
Anonimizzazione
Tracciabilità
Partizionamento
Archiviazione
Sicurezza dei documenti cartacei
Minimizzazione dei dati
Vulnerabilità

### Rischi

Accesso illegittimo ai dati
Modifiche indesiderate dei dati
Perdita di dati

Misure Migliorabili
Misure Accettabili

## 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

GIACOMO MARCHIONI

### Parere del DPO/RPD

Le finalità e le basi giuridiche del trattamento in essere sono chiaramente definite. Sono rispettati i principi di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione ed esattezza dei dati, limitazione della conservazione, integrità e riservatezza dei dati. Le misure di sicurezza soo adeguate.

### Richiesta del parere degli interessati

### Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

### Motivazione della mancata richiesta del parere degli interessati

Il parere degli interessati non è stato richiesto poichè il trattamento è obbligatorio in relazione all'esercizio dei pubblici poteri da parte dell'Ente attuatore.

## Contesto
### Panoramica del trattamento

### Quale è il trattamento in considerazione?

La DPIA ha per oggetto il trattamento dei dati personali acquisiti tramite la piattaforma informatica GLOBALeaks opensource inerente le segnalazioni di WHISTLEBLOWING

### Quali sono le responsabilità connesse al trattamento?

Titolare del Trattamento è ATER di Rieti - Via degli Olivi n.20- 00040520579 - Responsabile interno del Trattamento è il Dott. Stefano Beccarini - Il Responsabile esterno del Trattamento dei dati è la società WHISTLEBLOWING SOLUTION ai sensi dell'art. 28 GDPR.
Seeweb - Sub Responsabile del trattamento nominato da Whistlwblowing Solutions per la gestione del trattamento Iaas.

### Ci sono standard applicabili al trattamento?

ISO27001 - Erogazione di Servizi Saas di Whistleblowing Digitale su base Globaleaks.
ISO27017 controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud.
ISO 27'018 per la protezione dei dati personali nei servizi Public Cloud
Qualifica AGID
Certificazione CSA Star

**Valutazione : Accettabile**

## Contesto
### Dati, processi e risorse di supporto

### Quali sono i dati trattati?

Operazioni informatizzate di trattamento dei dati personali relative alla raccolta e conservazione dei dati necessari per l'erogazione dei servizi in modalità Saas così 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 è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

| | |
|---|---|
| **Ciclo di vita del trattamento e** | 1 Attivazione della piattaforma<br>2 Configurazione della piattaforma<br>3 Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi preposti |

| | |
|---|---|
| **dei dati** | parte dei riceventi preposti<br>4 Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge per finalità amministrative e contabili con coseguente 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**

## Principi Fondamentali

### Proporzionalità e necessità

### Gli scopi del trattamento sono specifici, espliciti e legittimi?

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.

**Valutazione : Accettabile**

### Quali sono le basi legali che rendono lecito il trattamento?

Obbligo di legge .

D. LGS. 231/2001

D.lgs n. 24/2023

Il trattamento ènecessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui è investito il tiolare del trattamento - ex art. 6 par.1 lettera e) Regolamento UE 2016/679.

**Valutazione : Accettabile**

### 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.

**Valutazione : Accettabile**

### 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 : Accettabile**

### Qual è 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**

## Principi Fondamentali

### Misure a tutela dei diritti degli interessati

### Come sono informati del trattamento gli interessati?

Informativa privacy ai sensi degli artt.li 13- 14 del Regolamento UE

**Valutazione : Accettabile**

### Ove applicabile: come si ottiene il consenso degli interessati?

Non applicabile. Obbligo di leggew

**Valutazione : Accettabile**

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

Pubblicità degli atti previsti dalla normativa sulla Trasparenza, Legge n. 241/90 e ss.mm.ii, Accesso Civico.
Il titolare ha definito procedure di riscontro - da art. 15 al 22 del GDPR

**Valutazione : Accettabile**

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

Artt.li 16 e 17 del GDPR

**Valutazione : Accettabile**

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

Articolo 21 EU RGPD "Diritto di opposizione"
L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni.

Informazion

**Valutazione : Accettabile**

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

Gli accordi contrattuali sono definiti con la società.

**Valutazione : Accettabile**

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

I dati non sono trasferiti al di fuori dell'UE

**Valutazione : Accettabile**

## 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.

**Valutazione : Accettabile**

### Anonimizzazione

No

**Valutazione : Accettabile**

### 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.

**Valutazione : Accettabile**

### Partizionamento

No partizionamento

**Valutazione : Accettabile**

### Archiviazione

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

**Valutazione : Accettabile**

### Sicurezza dei documenti cartacei

Il trattamento è definito da una procedura predisposta per il trattamento dei dati personali cartacei. Il Responsabile del Trattamento ha ricevuto isruzioni attraverso il contratto di nomina ai sensi dell'art 28 del GDPR

**Valutazione : Accettabile**

### Minimizzazione dei dati

Sono trattati solamenti i dati di cui il Titolare ha necessità per raggiungere le finalità del trattamento

**Valutazione : Accettabile**

### Vulnerabilità

L'applicativo GlobaLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base

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

**Valutazione : Accettabile**

# Rischi

## Accesso illegittimo ai dati

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

Applicazioni di sanzioni amministrative e penali - Ipotesi di richiesta del risarcimento del danno in sede civile

### Quali sono le principali minacce che potrebbero concretizzare il rischio?

Violazione dei protocolli per il trattamento dei dati cartaceo e informatico

### Quali sono le fonti di rischio?

Informatiche ( virus, perdita di dati, malware), Legate al fattore umano

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

Crittografia, Tracciabilità, Archiviazione, Minimizzazione dei dati, Sicurezza dei documenti cartacei, Vulnerabilità

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

Limitata, LIMITATO

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

Limitata,
Limitata consultazione del dati sensibili legati al WHISTLEBLOWING in relazione all'anonimità delle segnalazioni e alle garanzie prestate dal Responsabile per la prevenzione della Corruzione

**Valutazione : Accettabile**

# Rischi

## Modifiche indesiderate dei dati

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

Applicazioni di sanzioni amministrative e penali - Ipotesi di richiesta del risarcimento del danno in sede civile

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

Violazione dei protocolli per il trattamento dei dati cartaceo e informatico

### Quali sono le fonti di rischio?

### Quali sono le fonti di rischio?

Legate al fattore umano, Informatiche ( virus, perdita di dati, malware)

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

Crittografia, Anonimizzazione, Archiviazione, Sicurezza dei documenti cartacei, Vulnerabilità

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

Limitata, In relazione alle misure informatiche adottate e d alla tracciabilità degli accessi

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

Limitata, Anonimità delle segnalazioni e garanzia del Responsabile per la Prevenzione della Corruzione

**Valutazione : Accettabile**

# Rischi

## Perdita di dati

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

Applicazioni di sanzioni amministrative e penali - Ipotesi di richiesta del risarcimento del danno in sede civile

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

Violazione dei protocolli per il trattamento dei dati cartaceo e informatico

### Quali sono le fonti di rischio?

Informatiche ( virus, perdita di dati, malware), Legate al fattore umano

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

Crittografia, Anonimizzazione, Archiviazione, Sicurezza dei documenti cartacei, Vulnerabilità

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

Limitata, In relazione ai protocolli adottati.

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

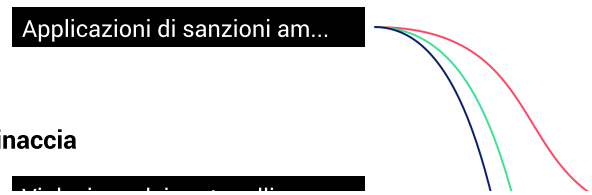
Limitata, L'esistenza di protocolli interni adottati dal Titolare del Trattamento e del Resposanbile del Trattamento esterno

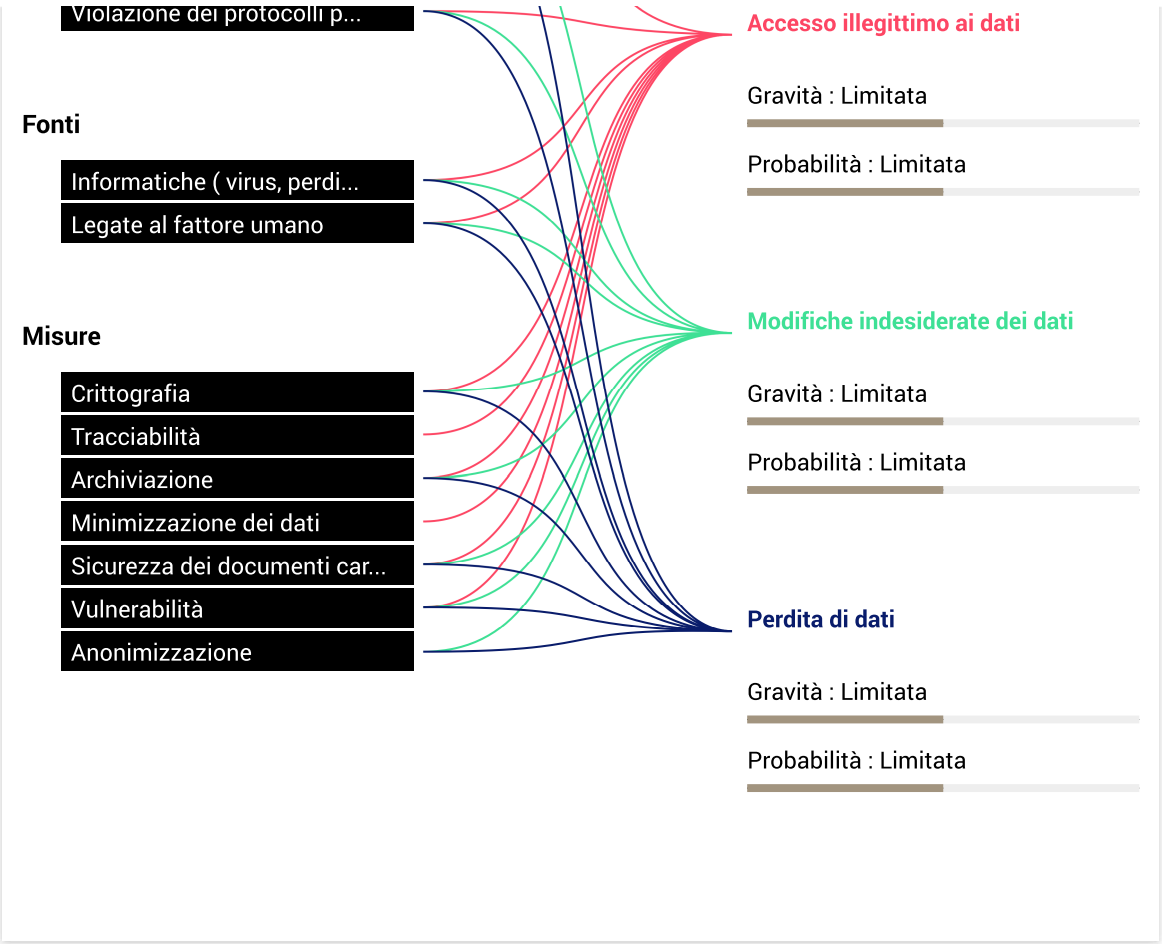
**Valutazione : Accettabile**

# Rischi

## Panoramica dei rischi

**Impatti potenziali**




Violazione dei protocolli p...
Fonti
Informatiche ( virus, perdi...
Legate al fattore umano
Misure
Crittografia
Tracciabilità
Archiviazione
Minimizzazione dei dati
Sicurezza dei documenti car...
Vulnerabilità
Anonimizzazione
Accesso illegittimo ai dati
Gravità : Limitata
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Limitata
Probabilità : Limitata
Perdita di dati
Gravità : Limitata
Probabilità : Limitata