

DOCUMENTAZIONE A SUPPORTO DEL TITOLARE PER LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

TRATTAMENTO DATI RELATIVI ALLE SEGNALAZIONI DI
CONDOTTE ILLECITE (C.D. WHISTLEBLOWING)

Documento aggiornato il 06 marzo 2024

SOMMARIO

1. PREMESSA	3
2. DESCRIZIONE DELLA PIATTAFORMA DI WHISTLEBLOWING	3
3. DESCRIZIONE E ANALISI DEL CONTESTO	6
4. VALUTAZIONI IN MERITO AI TRATTAMENTI	8
5. MISURE DI SICUREZZA	10
6. MISURE ADDIZIONALI	13

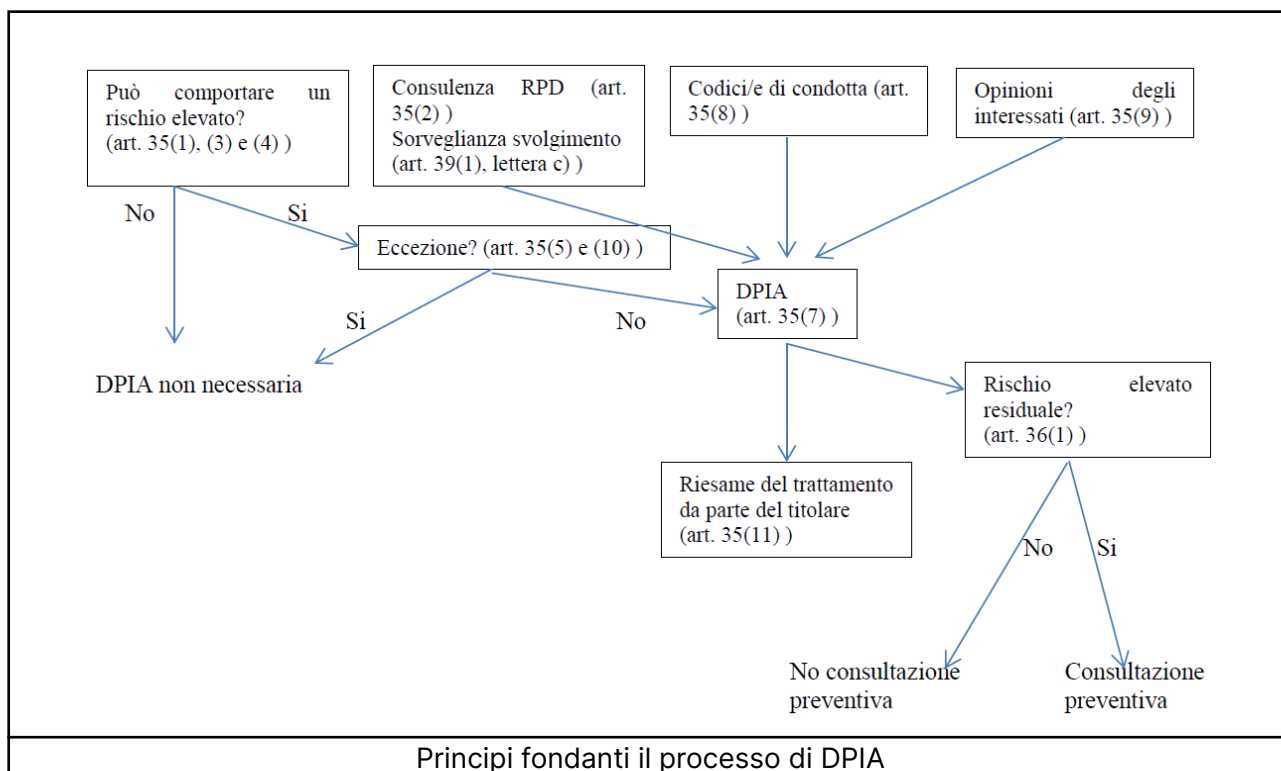
1. PREMESSA

La Valutazione d’Impatto sulla Protezione dei Dati (di seguito “DPIA) è un processo che il Titolare del trattamento deve effettuare, in via preventiva, ogni qual volta un trattamento di dati personali, in particolare connesso all’impiego di nuove tecnologie, in considerazione della natura, dell’oggetto, del contesto e delle finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone.

Il processo di DPIA è ritenuto uno degli aspetti di maggiore rilevanza nel nuovo quadro normativo definito dal Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679), in quanto esprime chiaramente la responsabilizzazione (c.d. accountability) del titolare nei confronti dei trattamenti dallo stesso effettuati.

Il Titolare del trattamento, infatti, è tenuto non solo a garantire l’osservanza delle disposizioni regolamentari, quanto anche a dimostrare adeguatamente in che modo egli garantisca tale osservanza.

Whistleblowing Solutions, nel suo ruolo di Responsabile del trattamento per la gestione del sistema di whistleblowing, con il presente documento intende fornire tutti gli elementi ai Titolari per svolgere la valutazione di impatto così come previsto dall’art. 35 del Regolamento.



2. DESCRIZIONE DELLA PIATTAFORMA DI WHISTLEBLOWING

Whistleblowing Solutions, in qualità di responsabile del trattamento, si occupa della gestione 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.

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 ed open-source [Globleaks](#) di cui Whistleblowing Solutions è co-autore e coordinatore di progetto.

In aggiunta a Globleaks, 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 versioni 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 differenti componenti secondo 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.

3. DESCRIZIONE E ANALISI DEL CONTESTO

<p>Responsabilità connesse al trattamento</p>	<p>PA, Ente o Organizzazione > Titolare del trattamento</p> <p>Gestore delle segnalazioni > Soggetto autorizzato dal Titolare del Trattamento a trattare i dati relativi alle segnalazioni</p> <p>Whistleblowing Solutions > Responsabile del trattamento per la fornitura e la gestione del sistema di whistleblowing</p> <p>Seeweb > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura (IaaS)</p> <p>Transparency International Italia > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing</p>
<p>Standard applicabili</p>	<p>Il contesto normativo di riferimento richiede conformità a:</p> <ul style="list-style-type: none"> ● D.Lgs. n. 24/2023 o altra normativa nazionale in caso di entità giuridiche con sede in altro Paese. ● DIRETTIVA (UE) 2019/1937 (WHISTLEBLOWING) ● GENERAL DATA PROTECTION REGULATION - 2016/679 (GDPR) <p>Il servizio erogato adotta misure progettate in aderenza allo standard internazionale ISO37002:2021 in materia di gestione dei processi di whistleblowing.</p> <p>Il Responsabile adotta un modello di gestione integrata dei propri processi di fornitura SaaS certificato:</p> <ul style="list-style-type: none"> ● ISO/IEC 27001:2022 ● ISO/IEC 27017:2015 ● ISO/IEC 27018:2019 ● ISO 9001:2015 ● CSA STAR Level 1 ● ACN

<p>Dati e operazioni di trattamento</p>	<p>Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per l'erogazione dei servizi in modalità SaaS così come pattuito tra le parti.</p> <p>Dati di registrazione</p> <p>Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (es. Responsabile Anticorruzione).</p> <p>Categorie particolari di dati</p> <p>Dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati.</p> <p>Dati relativi a condanne penali e reati</p> <p>Dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.</p>
<p>Ciclo di vita del trattamento e dei dati</p>	<ol style="list-style-type: none"> 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
<p>Risorse a supporto delle attività di trattamento</p>	<p>Software di whistleblowing professionale GlobalLeaks.</p> <p>Infrastruttura IaaS e SaaS privata basata su tecnologie:</p> <ul style="list-style-type: none"> - Dettaglio Hardware - VMWARE (virtualizzazione)

	<ul style="list-style-type: none">- Debian Linux LTS (sistema operativo)- VEEAM (backup)- OPNSENSE (firewall)- OPENVPN (vpn)
--	---

4. VALUTAZIONI IN MERITO AI TRATTAMENTI

PRINCIPI FONDAMENTALI

Adeguatezza, pertinenza e limitazione a quanto è necessario in relazione alle finalità per le quali i dati sono trattati (minimizzazione)	<p>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).</p> <p>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.</p> <p>Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo GlobalLeaks, 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.</p> <p>L'applicativo GlobalLeaks 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.</p>
--	--

Esattezza e aggiornamento dei dati	<p>L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata.</p> <p>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.</p>
Periodo di conservazione dei dati	<p>Policy di data retention di default delle segnalazioni di 12 mesi, con cancellazione automatica sicura delle segnalazioni che raggiungono la data di scadenza. Il gestore può anticipare la scadenza delle segnalazioni fino a 3 mesi dalla data dell'operazione e può prorogare la scadenza delle segnalazioni per il tempo ritenuto congruo al trattamento dei dati. Anticipazioni e proroghe delle scadenze possono essere fatte dal gestore più volte.</p> <p>Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma.</p>
Definizione degli obblighi dei responsabili del trattamento e formalizzazione dei contratti	<p>Gli accordi contrattuali sono definiti con le seguenti società:</p> <ul style="list-style-type: none">• 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

Protezione in caso di trasferimento di dati al di fuori dell'Unione europea:

I Dati Personali sono trattati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Europea.

Non esiste alcun trasferimento di Dati Personali verso l'estero in paesi extra UE.

5. MISURE DI SICUREZZA

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 [SSL Labs 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 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/main/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.

6. MISURE ADDIZIONALI

Il presente documento sintetizza una serie di metodologie standard conformi con la normativa vigente in ambito nazionale ed internazionale in materia di trattamento sicuro dell'informazione, privacy e whistleblowing.

A queste si aggiunge un crescente insieme altre misure al passo con la ricerca e la tecnica in ambito di sicurezza informatica reperibile alle seguenti pagine web:

- [THREAT MODEL](#)
- [APPLICATION SECURITY](#)