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)

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.

SOMMARIO

Documento aggiornato al 02/05/2025

1. PREMESSA

Il presente documento è destinato agli Enti che utilizzano l'applicativo per la gestione delle segnalazioni di whistleblowing reso disponibile in forma gratuita da ASMEL Associazione (di seguito, "ASMEL"), con l'obiettivo di fornire le informazioni necessarie alla redazione della Valutazione d'Impatto sulla Protezione dei Dati (DPIA – Data Protection Impact Assessment), in conformità a quanto previsto dall'art. 35 del Regolamento (UE) 2016/679 (GDPR).

Dal punto di vista operativo, il servizio è erogato da ASMENET Soc. Cons. a r.l., tra cui la gestione tecnica del sistema di whistleblowing, con riferimento all'esecuzione delle operazioni informatizzate di trattamento dei dati personali, relative alla raccolta, conservazione e gestione delle informazioni necessarie all'erogazione del servizio.

Pertanto, in relazione alle responsabilità connesse al trattamento dei dati relative Servizio di Whistleblowing, le stesse risultano così individuate:

- **TITOLARE DEL TRATTAMENTO**: l'Ente che utilizza il servizio
- **RESPONSABILE DEL TRATTAMENTO**: ASMEL Associazione
- **SUB-RESPONSABILE DEL TRATTAMENTO**: ASMENET S.C.aR.L.

2. DESCRIZIONE DELLA PIATTAFORMA DI WHISTLEBLOWING

ARCHITETTURA DI SISTEMA

L'architettura di sistema è principalmente composta da:

- Server virtualizzati su ambiente cloud sicuro Google Cloud Platform Ubuntu 24.04
- Sistema di gestione centralizzato per configurazione e monitoraggio

SOFTWARE IMPIEGATO

La piattaforma informatica di segnalazione è basata sul software libero ed 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:

- **Linux (Ubuntu Server)** – sistema operativo principale
- **NGINX** – reverse proxy e bilanciatore di carico
- **Python e Node.js** – gestione source code

Le limitate componenti software di natura proprietaria impiegate sono le seguenti:

- Google Cloud Virtualization

Predisposizione dei sistemi virtualizzati:

- Creazione di istanze virtuali in ambiente isolato
- Deploy automatizzato tramite script di provisioning
- Replica e snapshot periodiche per il ripristino di emergenza

ARCHITETTURA DI RETE

- Firewall hardware e software perimetrali con policy restrittive
- Connessioni cifrate (TLS/SSL) per tutte le comunicazioni di rete
- 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

STANDARD APPLICABILI

Il contesto normativo di riferimento richiede conformità a:

- 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)

Il servizio erogato adotta misure progettate in aderenza allo standard internazionale ISO 37002:2021.

Il Sub-Responsabile adotta un modello di gestione integrata dei propri processi di fornitura SaaS certificato:

- ISO/IEC 27001:2017

- ISO/IEC 27017:2015
- ISO/IEC 27018:2019
- ISO 9001:2015
- ISO 37001:2016
- ACN

DATI E OPERAZIONI DI TRATTAMENTO

Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per l'erogazione dei servizi.

DATI DI REGISTRAZIONE

Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (es. Responsabile Prevenzione della Corruzione).

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.

CICLO DI VITA DEL TRATTAMENTO E DEI DATI

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

RISORSE A SUPPORTO DELLE ATTIVITÀ DI TRATTAMENTO

Software di whistleblowing professionale GlobaLeaks. Infrastruttura SaaS privata basata su tecnologie:

- Linux (Ubuntu Server)
- NGINX
- Python e Node.js
- Google Cloud Virtualization

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)

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 questionari predisposti 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.

ESATTEZZA E AGGIORNAMENTO DEI DATI

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

PERIODO DI CONSERVAZIONE DEI DATI

I dati raccolti verranno conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. I dati verranno quindi conservati, ex lege dall'articolo 14 del Decreto legislativo n. 24, per un periodo di 5 anni dalla data di comunicazione dell'esito finale della procedura di segnalazione e comunque per tutta la durata dell'eventuale procedimento disciplinare, penale o dinanzi la Corte dei Conti

Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma.

DEFINIZIONE DEGLI OBBLIGHI DEI RESPONSABILI DEL TRATTAMENTO E

FORMALIZZAZIONE DEI CONTRATTI

Gli accordi contrattuali sono definiti:

- tra l'ENTE e ASMEL rispettivamente in qualità di Titolare e di Responsabile del trattamento
- tra ASMEL e ASMENET rispettivamente in qualità di Responsabile e Sub-Responsabile del trattamento

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 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

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.

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

È 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 Asmenet 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 del Sub-Responsabile 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 7:24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7:24.

I datacenter del fornitore IaaS sono certificati ISO27001

GESTIRE GLI INCIDENTI DI SICUREZZA E LE VIOLAZIONI DEI DATI PERSONALI

Il Sub-Responsabile ha definito una procedura per la gestione delle violazioni dei dati personali.

LOTTA CONTRO IL MALWARE

Tutti i computer del personale del Sub-Responsabile 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.