DUE ERRE IMPORT EXPORT S.R.L.

DPIA Canale interno di segnalazioni ex D. lgs. 24/2023

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: Iviquesse S.r.l.

Data di creazione: 17 dicembre 2023

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 preventiva di nessun parere agli Interessati, anche alla luce delle tutele previste dal canale e dalle modalità di gestione dello stesso.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento oggetto di valutazione della la presente DPIA riguarda la della raccolta delle segnalazioni whistleblowing attraverso il canale informatico adottato dall'azienda e fornito dalla società Iviquesse S.r.l., e la gestione delle segnalazioni stesse mediante i soggetti incaricati dalla predetta Società ("Gestore delle segnalazioni").

- La segnalazione è effettuata mediante la piattaforma disponibile al link https://dueerre.wb.scuadra.online/#/
- a richiesta della persona segnalante, mediante un incontro diretto con il Gestore delle segnalazioni

Quali sono le responsabilità connesse al trattamento?

Le segnalazioni sono trattate esclusivamente dal Gestore per le segnalazioni. Se si utilizza la piattaforma web sono coinvolti, per esclusive ragioni tecniche e di manutenzione, anche:

- **Iviquesse S.r.l.** > Responsabile del trattamento per la fornitura della piattaforma e la gestione delle segnalazioni di whistleblowing
- **Infoteam S.r.l.** > Sub-Responsabile del trattamento, nominato fornitore di Iviquesse s.r.l., per la fornitura e gestione dell'infrastruttura (Azure)
- **Microsoft Azure** > Sub-Responsabile del trattamento, fornitore di Infoteam S.r.l., quale Provider del Data Centre

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
- Reg UE 679/2016
- D. lgs. 24/2023

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 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:

- Installazione su piattaforma Microsoft Azure con ubicazione nella “Cloud Region” denominata “North Italy” e che consiste in 3 data-center fra loro ridondanti ubicati in Lombardia.
- Nr. 1 WatchGuard Firebox Cloud Small MSSP Appliance;
- Nr. 1 Virtual Machine Linux Ubuntu 22.04 LTS

  N. 1 1 D2a v4 (2 vCPUs, 8 GB RAM) x 720 Hours (Pay as you go), Linux, (Pay as you go); 1 managed disk – S6; Inter Region transfer type, 5 GB outbound data transfer from Italy North to West Europe N. 1 Basic (Classic), 0 Dynamic IP Addresses X 720 Hours, 1 Static IP Addresses X 730 Hours N. 1 Managed Disks, Standard HDD, S4 Disk Type 1 Disks, 100 Storage transactions; Pay as you go N. 1 Italy North (Virtual Network 1): 100 GB Outbound Data Transfer; West Europe (Virtual Network 2): 100 GB Outbound Data Transfer N. 1 1 A2 v2 (2 Cores, 4 GB RAM) x 720 Hours (Pay as you go), Linux, (Pay as you go); 0 managed disks – S4; Inter Region transfer type, 5 GB outbound data transfer from Italy North to East Asia

SOFTWARE IMPIEGATO

La piattaforma informatica di segnalazione è basata sul software libero ed open-source GlobaLeaks così come fornita, senza personalizzazioni che potenzialmente possano compromettere la sicurezza e le funzionalità.
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 seguenti tecnologie:

- open source:
    - Ubuntu/Linux (principale sistema operativo utilizzato);
    - Servizio di posta elettronica gestito da Register.it (mail server);
    - Servizio Register.it per il servizio DNS (dns server);
    - OpenVPN (vpn).

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

- Hyper-V in ambiente azure;
- RSync, software di backup;
- Watchguard (Firewall)

Predisposizione dei sistemi virtualizzati:

- La macchina virtuale viene gestita esclusivamente con sistemi Ubuntu/Linux nelle sole version Long Term Support (LTS);
- La macchina ha una lan "Azure" dedicata

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;
- La macchina virtuale istanziata viene esposta nella porta 80 e 443 per erogare i servizi
- 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; Vengono comunque predisposti degli archivi dove monitorare eventuali attacchi al sistema (Firewall Watchguard)
- 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 dal D. Lgs. 24/2023, gli illeciti o i fatti 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 al gestore della segnalazione 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. Sul punto si precisa che il segnalante può rimanere anonimo o rilasciare le proprie generalità.
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 nel sito della società, ed attraverso la procedura per poter effettuare la segnalazione. L'informativa è pubblicata all'interno del sito web istituzionale.

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

Si, 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:
● Ente gestore delle segnalazioni Iviquesse S.r.l.;
● Infoteam S.r.l.. in qualità di subResponsabile del trattamento nominato da Iviquesse S.r.l.
● Microsoft Azure > Sub-Responsabile del trattamento, nominato da Infoteam S.r.l., quale Provider del Data Center

I dati sono trasferiti al di fuori del territorio UE?

No. Anche i Data Centre si trovano all'interno dell'UE.

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 gestore delle segnalazioni;
- 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;
- Utilizzo della piattaforma IT per le segnalazioni e relative misure di sicurezza applicate alla stessa

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 gestore delle segnalazioni;
- 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;
- Utilizzo della piattaforma IT per le segnalazioni e relative misure di sicurezza applicate alla stessa

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 gestore delle segnalazioni;
- 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;
- Utilizzo della piattaforma IT per le segnalazioni e relative misure di sicurezza applicate alla stessa

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 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.
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.
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 giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery. Un disco viene montato all'interno del percorso ./globaleaks/backups sul quale vengono depositati i file di backup che viene effettuato due volte al giorno.

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 Iviquesse S.r.l. e/o Infoteam 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 Referente privacy di Iviquesse S.r.l.:

A seguito dell'analisi del documento, visto l'art. 39 par. 1 lett. C del Reg. 679/2016, si 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.

***

Castelfranco Veneto (TV), 16 Ottobre 2024