TeamSystem Whistleblowing

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

TeamSystem, 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.
Il software è conforme allo standard ISO 37002, alla direttiva UE 2019/1937 e al Decreto Legislativo italiano di attuazione n.24 del 10 marzo 2023.

Accordi per la protezione dei dati personali: https://www.teamsystem.com/dpa/

La piattaforma informatica di segnalazione è basata sul software TeamSystem Whistleblowing powered by GlobaLeaks.

MISURE DI SICUREZZA

CRITTOGRAFIA

L'applicativo implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing. 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.

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 supporta protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238.

TRACCIABILITÀ

L'applicativo 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 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

Globaleaks è periodicamente soggetto 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.

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 e per quelli che compongono l'infrastruttura fisica e di backup è prevista una modalità di manutenzione accessibile al personale TeamSystem e ai relativi fornitori, Smart Flow e Synesthesia, attraverso cui svolgere le modifiche al sistema e installare gli aggiornamenti.

SICUREZZA DEI CANALI INFORMATICI

Tutte le connessioni sono protette tramite protocollo TLS 1.2+ e connessioni con protocollo SSH.

SICUREZZA DELL' HARDWARE

I datacenter del fornitore 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.

Il fornitore di hosting è certificato ISO 9001:2015 e ISO 27001:2013.

GESTIRE GLI INCIDENTI DI SICUREZZA E LE VIOLAZIONI DEI DATI PERSONALI

TeamSystem ha definito una procedura per la gestione delle violazioni dei dati personali.

Privacy Policy: https://www.teamsystem.com/privacy-policy/

LOTTA CONTRO IL MALWARE

I computer del personale di TeamSystem e dei sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale e 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.

SUB - RESPONSABILI

- **Smart Flow Srl SB**
  P.IVA: 11592420019
  Corso Giuseppe Siccardi, 11 bis - 10122 Torino (TO)
  Sito web: https://smart-flow.it
  Configurazione dei portali Whistleblowing, assistenza clienti
- **Synesthesia Srl SB**
  P. IVA 10502360018
  Corso Dante, 118 - 10126 Torino (TO)
  Sito web: https://www.synesthesia.it
  Sviluppo e manutenzione software e hardware
- **Host.it**
  P.IVA 08505460017
  Corso Svizzera 185, 10149 Torino (TO)
  Sito web: https://host.it
  Servizio di hosting

TRASFERIMENTO DI DATI PERSONALI

Non viene effettuato alcun trasferimento di dati personali. In particolare i dati rimangono sul territorio italiano.

RIEPILOGO DELLE MISURA DI SICUREZZA FISICHE ADOTTATE

- Credenziali di autenticazione, assegnate individualmente ad ogni addetto.
    - Autenticazione mediante user-id e password.
    - Parola chiave di almeno 12 caratteri.
    - Disattivazione delle vecchie credenziali.
    - Disposizioni scritte per la disponibilità dei dati.
- Cifratura dei dati memorizzati.
- Cifratura dei dati trasmessi.
    - Cifratura con protocollo PGP.
- Sospensione automatica delle sessioni di lavoro.
- Sospensione manuale delle sessioni di Lavoro.
- Sono stati adottati adeguati criteri tra cui l'eventuale nomina a Responsabile per garantire che la struttura esterna presso cui l'unità di archiviazione risiede abbia adeguate contromisure che garantiscano un rischio residuale basso.
- Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda
- Verifica ed eventuale nomina degli amministratori di sistema se presenti
- Pseudonimizzazione.
- Trattamento dei dati con protocolli criptati.
- Profili di autorizzazione di ambito diverso per diversi incaricati.
    - È utilizzato un sistema di autorizzazione.
    - I profili di autorizzazione vengono specificati prima di ogni trattamento.
    - Verifica periodica del profilo di autorizzazione.