Comune di Mariano Comense

Data Protection Impact Assessment

Sul trattamento dei dati per la gestione delle segnalazioni di whistleblowing

Versione 1.0 (30.11.2023)

Redatta da: Elena Imi, Gianpietro Turani

Verificata da: Mattia Cortinovis

Validata da: Claudia La Rosa

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento preso in considerazione nella presente DPIA è quello effettuato dal Comune di Mariano Comense per la gestione delle segnalazioni di "Whistleblowing" ai sensi del D.Lgs. 24/2023.

Quali sono le responsabilità connesse al trattamento?

Il titolare del trattamento è il Comune di Mariano Comense.

Whistleblowing Solutions I.S. S.r.l. è responsabile del trattamento poiché fornisce il servizio di fornitura in outsourcing di una piattaforma di whistleblowing digitale.

Transparency International Italia è sub-responsabile del trattamento perché fornisce il servizio di supporto agli utenti e di amministrazione di sistema.

Seeweb S.r.l. è sub-responsabile del trattamento perché fornisce il servizio di archiviazione e hosting in cloud.

L'autorizzato al trattamento (gestore) è il Segretario comunale/RPCT

Ci sono standard applicabili al trattamento?

Gli standard applicabili derivano dalle seguenti fonti:

- Direttiva UE 2019/1937, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione;
- D.lgs. n. 24/2023 "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;
- Regolamento UE n. 2016/679 (c.d. GDPR)
- D.lgs. n. 196/2003 (c.d. Codice Privacy) così come modificato dal D.lgs. n. 101/2018;
- Linee Guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali, approvate da ANAC con Delibera 311 del 12 Luglio 2023;
- Parere dell'Autorità Garante per la protezione dei dati personali (provvedimento n. 304 del 6 luglio 2023)

Valutazione: Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Nell'ambito della gestione delle segnalazioni di whistleblowing possono essere gestiti:

- Dati anagrafici (nome, cognome, ecc.);

- Dati di contatto (numero di telefono, indirizzo mail);
- Dati identificativi;
- Dati relativi ai rapporti professionali;
- Dati finanziari e patrimoniali;
- Dati relativi ai reati oggetto della segnalazione;
- Eventuali altri dati (anche particolari) che, pur non espressamente richiesti dal titolare, siano contenuti nelle segnalazioni ricevute.

Gli interessati sono:

- I soggetti che effettuano la segnalazione ("segnalanti"), se decidono di fornire propri dati personali;
- I soggetti a cui si riferisce la segnalazione ("segnalati"), e sui quali potrebbero essere svolte ulteriori indagini per accertare la loro eventuale responsabilità;
- Eventuali ulteriori soggetti citati nella segnalazione;
- I soggetti incaricati dal Titolare alla gestione delle segnalazioni ("Gestori").

Valutazione: Accettabile

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

I dati sono inizialmente raccolti quando il titolare riceve una segnalazione di whistleblowing, ed eventualmente possono essere integrati nel corso delle successive attività istruttorie.

Il canale di segnalazione è la piattaforma online dedicata al whistleblowing ("piattaforma"), che si avvale del software GlobaLeaks. La piattaforma è accessibile da chiunque tramite internet, ed è linkata dal sito del titolare.

La segnalazione avviene con le seguenti modalità**:** dopo essersi collegato alla piattaforma, il segnalante viene guidato nella compilazione di un questionario scritto formato da domande aperte e/o chiuse che gli permetteranno di fornire gli elementi caratterizzanti della segnalazione (fatti, soggetti coinvolti, contesto temporale, luogo, ecc.). La piattaforma consente inoltre al segnalante di fissare un incontro di persona con il gestore.

La piattaforma offrirà al segnalante la scelta se rivelare o meno la propria identità. In ogni caso il segnalante potrà eventualmente fornire le proprie generalità in un secondo momento, sempre attraverso la piattaforma.

Nel momento dell'invio della segnalazione, la piattaforma rilascerà al segnalante un codice identificativo univoco: tale codice, conosciuto esclusivamente dal segnalante, non potrà essere recuperato in alcun modo in caso di smarrimento. Il codice servirà al segnalante per accedere, sempre tramite il Portale, alla propria segnalazione al fine di monitorarne lo stato di avanzamento, inserire ulteriori elementi utili a circostanziare la segnalazione, rispondere ad eventuali domande di approfondimento poste dal gestore. La piattaforma consente, infatti, di instaurare un colloquio virtuale (chat) tra segnalante e gestore.

La piattaforma non invierà al segnalante notifiche di alcun tipo, al fine di tutelare più efficacemente la sua identità.

Quando viene inviata una segnalazione, il gestore ne riceve notifica tramite un messaggio di posta elettronica sulla propria casella mail. Tale messaggio non contiene alcuna informazione sul segnalante o sul contenuto della segnalazione (dati che restano esclusivamente sula piattaforma).

Il Gestore accede al contenuto della segnalazione loggandosi sulla piattaforma (con proprie credenziali dedicate).

Le segnalazioni ritenute palesemente infondate verranno archiviate.

Negli altri casi, il gestore provvede:

- ad avviare approfondimenti e accertamenti specifici avvalendosi, se ritenuto opportuno, delle strutture competenti del Comune di Mariano Comense o di esperti esterni, sempre evitando di rivelare dati personali se non strettamente necessari ai fini dell'indagine;
- una volta completati i propri accertamenti, a sottoporre i risultati della propria valutazione ai soggetti competenti, affinché vengano intrapresi i più opportuni provvedimenti (ad esempio provvedimenti disciplinari, azioni giudiziarie, risoluzione di contratti, predisposizione di piani di azione per la rimozione delle debolezze di controllo rilevate);
- a concludere l'istruttoria in qualunque momento se, nel corso dell'istruttoria medesima, sia accertata l'infondatezza della segnalazione.

Tali attività non saranno necessariamente svolte nell'ordine di cui sopra, essendo libero il gestore, sotto la propria responsabilità, di individuare le priorità di intervento.

Le segnalazioni pervenute tramite canali diversi dal Portale Whistleblowing (es. posta ordinaria) saranno protocollate in un apposito registro riservato, a cura del gestore, e seguiranno il medesimo iter istruttorio. Qualora possibile, i segnalanti che abbiano utilizzato canali alternativi verranno indirizzati - per loro maggior tutela - all'utilizzo della piattaforma.

Valutazione: Migliorabile

Commento di valutazione: attualmente non è possibile effettuare la segnalazione mediante linee telefoniche o sistemi di messaggistica vocale. Resta fermo che il segnalante può concordare un incontro di persona con il gestore ed esporre verbalmente la propria segnalazione in tale sede.

Quali sono le risorse di supporto ai dati?

Piattaforma online:

Portale per il whistleblowing basata sul software GlobaLeaks.

Ambiente client:

Personal Computer usati dal gestore del Comune di Mariano Comense per accedere alla piattaforma.

Ambiente server:

CLOUD PROVIDER

L'ambiente server è ospitato presso i DataCenter del Cloud Provider Seeweb (Sub-responsabile del trattamento) i quali sono collocati sul territorio italiano e in paesi dell'Unione Europea. Seeweb possiede le certificazioni elencate alla pagina web https://www.seeweb.it/azienda/certificazioni. Tra queste si segnalano quelle più pertinenti all'ambito tecnico: ISO 22301 (continuità operativa), ISO 27001 (sicurezza delle informazioni) con le estensioni 27017 (sicurezza delle informazioni nel cloud) e 27018 (protezione dei dati personali nel cloud). Inoltre, sono presenti le certificazioni di ACN QI1 (per l'infrastruttura) e QC1 (per il servizio cloud IaaS), e la certificazione CSA STAR Level 1.

SERVICE PROVIDER

L'ambiente server è definito da Whistleblowing Solutions ed è costituito da un'architettura a strati così caratterizzati:

- Livello **fisico**: ambiente server computazionale implementato da un cluster di macchine dedicate; ambiente server di storage implementato da un apparato SAN (Storage Area Network) ridondato.
- Livello di **virtualizzazione**: realizzato mediante la tecnologia VMware
- Livello di **sistema operativo**: sistema Linux, distribuzione Debian LTS (Long Time Support)
- Livello **middleware**: mail server, dns server, firewall locali standard e integrate nel Sistema operativo
- Livello **applicativo**: piattaforma software GlobaLeaks scomposta in
  - BackEnd, implementato in python che offre API REST;
  - FrontEnd, implementato in tecnologia WEB (Html e Javascript) con l'impiego di framework considerati standard de-facto (Angular, Bootstrap). Il FrontEnd interagisce con il BackEnd mediante invocazione sicura dell'API REST esposta.
- Backup: implementato mediante la tecnologia Veeam

Rete:

La rete, su cui opera l'ambiente server sopra descritto, è isolata e protetta attraverso dispositivi di sicurezza perimetrale (apparati firewall in configurazione ad alta affidabilità) i quali consentono accessi alla parte applicativa sulla base di protocolli sicuri standard. Internamente all'infrastruttura server, la rete è segmentata in VLAN (Virtual LAN) sulla base di criteri di partizionamento orientati alle prestazioni e alla sicurezza.

L'accesso diretto ai server è possibile solo a personale competente dotato di adeguati privilegi amministrativi attraverso una VPN.

Personale:

il Gestore è il Segretario Comunale/RPCT del Comune di Mariano Comense, autorizzato al trattamento dei dati per la gestione delle segnalazioni.

Valutazione: Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Lo scopo del trattamento è esplicitamente definito, e consiste nella gestione delle segnalazioni di whistleblowing. Lo scopo è legittimo, essendo un adempimento obbligatorio imposto dalla legge.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica del trattamento è la necessità dello stesso per adempiere a un obbligo di legge (D.Lgs. 24/2023).

Nel caso specifico dei trattamenti previsti dagli artt. 12 e 14 del D.lgs. n. 24/2023 (rivelazione dell'identità dell'interessato, o registrazione/verbalizzazione della segnalazione presentata con messaggio vocale o durante un incontro personale) la base giuridica è il consenso dell'interessato.

Se necessario al fine dell'adozione dei provvedimenti conseguenti alla segnalazione e, in generale, per la tutela dei diritti del Titolare, la base giuridica dei relativi trattamenti è il legittimo interesse del Titolare.

Il trattamento di dati particolari potrà avvenire esclusivamente qualora gli stessi siano necessari e pertinenti alla segnalazione; in tal caso il trattamento è consentito per motivi di interesse pubblico rilevante (nello specifico, l'interesse a che siano rispettate le previsioni del D.lgs. n. 24/2023) e/o per la sua necessità al fine di accertare, esercitare o difendere un diritto in sede giudiziaria.

Il trattamento di dati relativi a condanne penali e ai reati o a connesse misure di sicurezza potrà avvenire esclusivamente qualora gli stessi siano necessari e pertinenti alla segnalazione; in tal caso il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri (in particolare dal D.lgs. n. 24/2023).

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)?

Il questionario proposto al segnalante richiede solo le informazioni utili per la gestione della segnalazione di whistleblowing. Per i dati non strettamente indispensabili – ma che comunque possono coadiuvare il gestore nello svolgimento dei propri compiti – il conferimento è lasciato alla discrezione del segnalante.

Data la natura aperta delle segnalazioni, è possibile che siano ricevuti dati superflui: in tal caso il gestore eviterà di acquisirli o procederà alla loro cancellazione. Nei casi in cui sussistano dubbi sulla pertinenza dei dati rispetto alla segnalazione, il gestore evita qualsiasi loro trattamento eccetto la conservazione sino alla chiusura della segnalazione (conservazione ammessa data la difficoltà di valutare con certezza l'inutilità di un dato mentre sono ancora in corso gli accertamenti, e la necessità di documentare la correttezza delle attività di gestione della segnalazione).

La piattaforma di whistleblowing è configurata per evitare la raccolta di dati tecnici idonei a rivelare l'identità del segnalante, quali per esempio indirizzi IP, User Agents e altri Metadati.

Valutazione: Accettabile

I dati sono esatti e aggiornati?

L'esattezza e l'aggiornamento dei dati ricevuti tramite la segnalazione iniziale non può essere garantita (dipendendo dalla diligenza del segnalante) ma è verificata nel corso degli accertamenti svolti dal gestore. La piattaforma di whistleblowing consente al segnalante di inviare (di propria iniziativa o su richiesta del gestore) nuove comunicazioni e documenti che possono correggere, integrare o aggiornare le informazioni inizialmente fornite.

Il titolare, in ogni caso, non intraprende iniziative esclusivamente in base ai dati ricevuti con la segnalazione, ma si attiene all'esito dell'istruttoria del gestore.

Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

Come previsto dall' art. 14 del D.Lgs. 24/2023, i dati sono conservati 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.

Decorsi i termini di conservazione sopra indicati, i dati saranno distrutti, cancellati o resi anonimi, compatibilmente con le tempistiche tecniche di cancellazione e backup.

Valutazione: Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Un'informativa specifica sul trattamento di whistleblowing viene fornita agli interessati mediante:

- La pubblicazione dell'informativa nella pagina del sito del titolare dedicata al whistleblowing;
- La consegna dell'informativa ai dipendenti e collaboratori del titolare nell'ambito delle iniziative di formazione e sensibilizzazione sul tema del whistleblowing;
- Per il futuro, la consegna dell'informativa ai dipendenti e collaboratori del titolare al momento dell'instaurazione del rapporto.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Poiché il consenso è richiesto solo in circostanze limitate (rivelazione dell'identità dell'interessato, o registrazione/verbalizzazione della segnalazione presentata durante un incontro personale), che potrebbero non verificarsi nella maggior parte delle segnalazioni, il consenso viene richiesto dal gestore caso per caso, qualora ciò si riveli necessario.

Il gestore raccoglie il consenso mediante una richiesta dedicata, che sottopone all'interessato e che conserva insieme agli altri documenti relativi alla pratica.

Il consenso può essere revocato rivolgendosi al gestore o, a discrezione dell'interessato, al DPO del titolare.

Valutazione: Accettabile

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

Gli interessati possono esercitare i propri diritti rivolgendosi, a loro discrezione, al gestore o al DPO del titolare. Nel primo caso l'interessato (se è il segnalante) può inviare la richiesta mediante i medesimi canali di comunicazione usati per la segnalazione. Nel secondo caso può utilizzare i contatti indicati nell'informativa.

Se la richiesta è ricevuta dal gestore, questi può avvalersi della collaborazione del DPO, evitando tuttavia di rivelargli informazioni (come l'identità dell'interessato) che non siano strettamente necessarie per riscontrare correttamente la richiesta.

L'esercizio dei diritti dell'interessato avviene nei limiti stabiliti dall'art. 13 del D.Lgs. 24/2023 e dall'art. 2-undecies del D.Lgs. 196/2003. Pertanto, i diritti non possono essere esercitati con richiesta al titolare del trattamento, ovvero con reclamo ai sensi dell'articolo 77 del GDPR, qualora dal loro esercizio possa derivare un pregiudizio effettivo e concreto, tra l'altro, alla riservatezza dell'identità del segnalante, o allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria conseguenti alla segnalazione. In tali casi, il titolare provvede comunque a riscontrare la richiesta dell'interessato, nei limiti in cui ciò sia possibile senza pregiudicare le esigenze di cui all'art. 2-undecies del D.Lgs. 196/2003. L'interessato potrà comunque rivolgersi all'Autorità Garante con le modalità previste dall'art. 160 del D.Lgs. 196/2003.

Con riferimento specifico al diritto di portabilità dei dati, lo stesso risulta non applicabile perché non ricorrono i presupposti di cui all'art. 20 del GDPR, fermo restando che tutte le richieste degli interessati saranno prese in considerazione e valutate nel merito.

Valutazione: Accettabile

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

Gli interessati possono esercitare i propri diritti rivolgendosi, a loro discrezione, al gestore o al DPO del titolare. Nel primo caso l'interessato (se è il segnalante) può inviare la richiesta mediante i medesimi canali di comunicazione usati per la segnalazione. Nel secondo caso può utilizzare i contatti indicati nell'informativa.

Se la richiesta è ricevuta dal gestore, questi può avvalersi della collaborazione del DPO, evitando tuttavia di rivelargli informazioni (come l'identità dell'interessato) che non siano strettamente necessarie per riscontrare correttamente la richiesta.

L'esercizio dei diritti dell'interessato avviene nei limiti stabiliti dall'art. 13 del D.Lgs. 24/2023 e dall'art. 2-undecies del D.Lgs. 196/2003. Pertanto, i diritti non possono essere esercitati con richiesta al titolare del trattamento, ovvero con reclamo ai sensi dell'articolo 77 del GDPR, qualora dal loro esercizio possa derivare un pregiudizio effettivo e concreto, tra l'altro, alla riservatezza dell'identità del segnalante, o allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria conseguenti alla segnalazione. In tali casi, il titolare provvede comunque a riscontrare la richiesta dell'interessato, nei limiti in cui ciò sia possibile senza pregiudicare le esigenze di cui all'art. 2-undecies del D.Lgs. 196/2003. L'interessato potrà comunque rivolgersi all'Autorità Garante con le modalità previste dall'art. 160 del D.Lgs. 196/2003.

Valutazione: Accettabile

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

Gli interessati possono esercitare i propri diritti rivolgendosi, a loro discrezione, al gestore o al DPO del titolare. Nel primo caso l'interessato (se è il segnalante) può inviare la richiesta mediante i medesimi canali di comunicazione usati per la segnalazione. Nel secondo caso può utilizzare i contatti indicati nell'informativa.

Se la richiesta è ricevuta dal gestore, questi può avvalersi della collaborazione del DPO, evitando tuttavia di rivelargli informazioni (come l'identità dell'interessato) che non siano strettamente necessarie per riscontrare correttamente la richiesta.

L'esercizio dei diritti dell'interessato avviene nei limiti stabiliti dall'art. 13 del D.Lgs. 24/2023 e dall'art. 2-undecies del D.Lgs. 196/2003. Pertanto, i diritti non possono essere esercitati con richiesta al titolare del trattamento, ovvero con reclamo ai sensi dell'articolo 77 del GDPR, qualora dal loro esercizio possa derivare un pregiudizio effettivo e concreto, tra l'altro, alla riservatezza dell'identità del segnalante, o allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria conseguenti alla segnalazione. In tali casi, il titolare provvede comunque a riscontrare la richiesta dell'interessato, nei limiti in cui ciò sia possibile senza pregiudicare le esigenze di cui all'art. 2-undecies del D.Lgs. 196/2003. L'interessato potrà comunque rivolgersi all'Autorità Garante con le modalità previste dall'art. 160 del D.Lgs. 196/2003.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato?

Non applicabile, poiché non sono prese decisioni basate unicamente su trattamenti automatizzati.

Valutazione: Accettabile

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

Sì, gli obblighi del responsabile del trattamento sono dettagliatamente disciplinati mediante appositi documenti contrattuali (nomina a responsabile).

Valutazione: Accettabile

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

Non applicabile, poiché i dati non sono trasferiti al di fuori dell'Unione Europea.

Valutazione: Accettabile

Misure di sicurezza

Misure esistenti o pianificate

Misure applicate ai dati

Crittografia

L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'ente americano OTF (Open Technology Fund). Ogni informazione scambiata tra l'applicativo e gli utilizzatori viene protetta in transito da protocollo TLS 1.2+ configurato conformemente a un rating A+ secondo SSL Labs. Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica. Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento o gestione nella piattaforma GlobaLeaks. Dettagli su questo aspetto si possono trovare alla pagina https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html.

Valutazione: Accettabile

Anonimizzazione

L'applicativo GlobaLeaks abilita la possibilità di navigazione tramite Tor Browser per finalità di accesso anonimo con garanzie corrispondenti allo stato dell'arte della ricerca tecnologica in materia. La segnalazione non richiede obbligatoriamente dati personali e al contrario rilascia un codice di 16 cifre che solo il segnalante conosce.

Valutazione: Accettabile

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. La password deve essere composta di almeno 12 caratteri e contenere una varietà di caratteri, tra cui almeno una lettera minuscola, una lettera maiuscola, un numero e un carattere speciale. Il sistema utilizza l'autenticazione a due fattori con protocollo TOTP (Time-based one-time password) secondo lo standard RFC 6238.

Valutazione: Accettabile

Minimizzazione dei dati

Nel rispetto del principio di privacy by design, tutti i componenti utilizzati (tra cui l'applicativo GlobaLeaks, i log di sistema, il 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 suggerisce la navigazione tramite Tor Browser per finalità di accesso completamente anonimo.

Valutazione: Accettabile

Sicurezza dei documenti cartacei

Non applicabile, poiché il trattamento avviene integralmente tramite una piattaforma informatica.

Valutazione: -

Tracciabilità (misure applicate ai dati)

L'applicativo GlobaLeaks implementa un sistema di log sicuro atto a registrare le attività effettuate dal gestore delle segnalazioni e dagli amministratori dal sistema. I log delle attività del segnalante sono privi delle informazioni identificative quali indirizzi IP e User Agent.

Valutazione: Accettabile

Archiviazione

L'applicativo GlobaLeaks utilizza un database relazionale (SQLite) a cui accede tramite una libreria ORM (Object-Relational Mapping). Le configurazioni effettuate forniscono elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità di sicurezza del database. Le segnalazioni e i relativi documenti sono conservati per un periodo di 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione. Al termine di tale periodo i dati sono cancellati automaticamente.

Valutazione: Accettabile

Misure generali di sicurezza dei sistemi

Gestione delle vulnerabilità

L'applicativo GlobaLeaks è periodicamente soggetto ad audit di sicurezza indipendenti su base almeno annuale, realizzati dallo sviluppatore del software. Tutti le risultanze sono pubblicate e sono sottoposte a revisione. A questa si aggiunge la revisione indipendente realizzata dalla 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 di sviluppo privatamente. L'attività di audit è documentata alla pagina https://docs.globaleaks.org/en/main/security/PenetrationTests.html dove sono scaricabili i report di Penetration Test. Vengono inoltre adottate tutte le misure di sicurezza per la prevenzione delle vulnerabilità, IPS e DDoS.

Valutazione: Accettabile

Tracciabilità (misure generali di sicurezza dei sistemi)

L'organizzazione è dotata di una policy formale sulla gestione dei data breach e degli incidenti di sicurezza; viene utilizzato un apposito registro per tracciare tali eventi e per valutare il livello di

rischio in conformità alle linee guida di ENISA (Recommendations for a methodology of the assessment of severity of personal data breaches).

Valutazione: Accettabile

Backup

I sistemi sono soggetti a backup locale e remoto giornaliero con retention di 7 giorni. La tecnologia scelta è Veeam Backup la quale consente di utilizzare i backup anche per finalità di disaster recovery.

Valutazione: Accettabile

Controllo degli accessi fisici

I datacenter di Seeweb sono dotati di un rigoroso controllo degli accessi, di procedure di monitoraggio e di videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche. I datacenter, come indicato, sono certificati in vario modo (in particolare secondo la ISO 27001 e le estensioni 27017 e 27018).

Valutazione: Accettabile

Sicurezza dei canali informatici

Ogni informazione scambiata tra l'applicativo e gli utilizzatori viene protetta in transito da protocollo TLS 1.2+ configurato conformemente a un rating A+ secondo SSL Labs. Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica.

Valutazione: Accettabile

Prevenzione delle fonti di rischio umane e non umane

I dati personali sono trattati esclusivamente nel territorio dell'Unione Europea e non sono trasmessi all'esterno di esso. I data center sono protetti nei confronti degli eventi fisici, tra i quali anche le catastrofi naturali (es. incendio, alluvione, terremoto, etc.).

Valutazione: Accettabile

Gestione postazioni

Le postazioni impiegate dagli operatori per interagire con l'applicazione GlobaLeaks sono dotate di antivirus con caratteristiche enterprise, ricevono il patching di sicurezza proposto dal sistema operativo, sono interessate da meccanismi di software distribution automatici e controllati. Il traffico generato dalle postazioni è intercettato dal modulo di content filtering del firewall dell'ente.

Valutazione: Migliorabile

Commento di valutazione: le postazioni non sono dotate di un sistema di cifratura del disco locale

Lotta contro il malware

Il PC del gestore è dotato di antivirus come da policy di sicurezza dell'ente, ed il gestore riceve periodicamente formazione in materia di sicurezza informatica.

Valutazione: Accettabile

Sicurezza dei siti web

La piattaforma Globaleaks implementa le Linee guida di sicurezza OWASP. Il sistema assegna una Sessione ad ogni utente autenticato. L'ID sessione è una chiave privata lunga 256 bit generata casualmente dal backend. Ogni sessione scade di conseguenza con un timeout di 60 minuti. Gli ID di sessione vengono scambiati dal client con il backend tramite un header (X-Session) e scadono non appena gli utenti chiudono il browser. Gli utenti possono disconnettersi esplicitamente tramite un pulsante di disconnessione o implicitamente chiudendo il browser. Viene evitato l'utilizzo di cookie per ridurre al minimo gli attacchi XSRF e ogni possibile attacco basato su di essi. L'autenticazione si basa invece su un'intestazione di sessione HTTP personalizzata inviata dal client su richieste autenticate.

Valutazione: Accettabile

Manutenzione

L'infrastruttura server-hardware è definita da Whistleblowing Solutions che ne cura la manutenzione di concerto con il Cloud Provider Seeweb. La contiuità di servizio è garantita mediante tecniche manutentive che fanno leva sulla ridondanza degli apparati.

Valutazione: Accettabile

Contratto con il responsabile del trattamento

I rapporti con il responsabile del trattamento (e tra questi e i sub-responsabili) sono formalizzati mediante appositi contratti e atti di nomina conformi all'art. 28 del GDPR.

Valutazione: Accettabile

Sicurezza dell'hardware

Il tema della sicurezza dell'hardware è risolto dalle misure di sicurezza implementate dal Cloud Service Provider ed evidenziate dai livelli di certificazione da esso posseduti.

Valutazione: Accettabile

Misure organizzative

Politica di tutela della privacy

È implementato un sistema di gestione della normativa privacy, in cui sono chiaramente definiti i ruoli e le responsabilità dei soggetti coinvolti (titolare, DPO, autorizzati al trattamento, responsabili del trattamento, ecc.).

Valutazione: Accettabile

Gestione delle politiche di tutela della privacy

Il sistema privacy è gestito tramite politiche e documenti formalizzati.

Valutazione: Accettabile

Gestione dei rischi; Vigilanza sulla protezione dei dati

L'organizzazione svolge un'analisi del rischio sui trattamenti effettuati; con specifico riferimento al trattamento di whistleblowing, il rischio viene valutato tramite la presente DPIA.

Valutazione: Accettabile

Integrare la protezione della privacy nei progetti

La presente DPIA viene realizzata contestualmente alla progettazione e implementazione del canale di whistleblowing, per assicurare che il nuovo trattamento sia conforme alla normativa in materia di protezione dei dati personali.

Valutazione: Accettabile

Gestire gli incidenti di sicurezza e le violazioni dei dati personali; Gestione dei terzi che accedono ai dati

L'organizzazione è dotata di una policy formale sulla gestione dei data breach e degli incidenti di sicurezza; viene utilizzato un apposito registro per tracciare tali eventi e per valutare il livello di rischio in conformità alle linee guida di ENISA (Recommendations for a methodology of the assessment of severity of personal data breaches).

Valutazione: Accettabile

Gestione del personale

Il personale coinvolto nelle attività di trattamento dei dati è stato formato sia sulla normativa privacy, sia su quella relativa al whistleblowing, nonché sulle modalità di funzionamento della piattaforma online e sulle corrette modalità di gestione delle segnalazioni. Sono previste iniziative periodiche di formazione e sensibilizzazione.

Valutazione: Accettabile

Rischi

Accesso illegittimo ai dati

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

Con riferimento ai dati del segnalante, la loro diffusione non autorizzata potrebbe comportare il rischio della sua identificazione e di conseguenti ritorsioni (comunque vietate dalla legge, e dalle policy interne del Titolare). Inoltre, qualora la segnalazione risultasse infondata, la perdita di riservatezza dei dati del segnalante potrebbe comportare una lesione della sua reputazione.

Con riferimento ai dati del segnalato, la loro diffusione non autorizzata comporterebbe una lesione della sua reputazione, e il rischio di difficoltà nel trovare posti di lavoro alternativi.

Con riferimento ai dati del gestore, trattandosi di informazioni per la maggior parte pubbliche, la loro diffusione non dovrebbe comportare conseguenze significative.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

- Attacco informatico finalizzato alla sottrazione dei dati
- Errore tecnico nell'attribuzione di permessi agli utenti
- Errore umano nella corretta gestione e conservazione dei dati
- Sottrazione manuale dei dati

Quali sono le fonti di rischio?

- Fonti umane esterne – criminali informatici
- Fonti umane interne – autorizzati al trattamento e amministratori negligenti
- Fonti umane interne – autorizzati al trattamento e amministratori infedeli

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Le misure rilevanti che contribuiscono alla mitigazione del rischio sono indicate a pagina 19 (tipologia riservatezza).

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

Importante.

Gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative.

L'impatto potenziale, pur mitigato dalle misure di sicurezza adottate (inclusa la possibilità per il segnalante di mantenere l'anonimato), non è completamente eliminabile, data la delicatezza dei dati oggetto di trattamento.

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

Limitata.

Appare difficile che le fonti di rischio considerate concretizzino una minaccia.

La probabilità di un concretizzarsi del rischio risulta efficacemente ridotta dalle misure di sicurezza adottate. Un'ulteriore diminuzione della probabilità deriva dalle previsioni di legge (e dalle politiche

dell’ente) volte a sanzionare sia condotte ritorsive illecite, sia segnalazioni diffamatorie proposte in mala fede (ovvero le conseguenze più dannose e verosimili di una violazione della riservatezza).

Valutazione: Accettabile

Modifiche indesiderate dei dati

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

Con riferimento ai dati del segnalante, eventuali violazioni dell'integrità del dato (se non accompagnate da violazione della riservatezza, per le quali si rinvia al paragrafo precedente) non dovrebbero avere conseguenze significative.

Con riferimento ai dati del segnalato e del gestore, delle modifiche indesiderate potrebbero invece avere conseguenze apprezzabili, poiché potrebbero portare a provvedimenti disciplinari o iniziative giudiziarie infondate.

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

- Errore degli utenti nel caricamento e nella gestione manuale dei dati
- Falsificazione dolosa dei dati
- Mancato aggiornamento di dati obsoleti
- Corruzione dei dati in conseguenza di bug nel software o problemi di funzionamento dell'hardware

Quali sono le fonti di rischio?

- Fonti umane interne – autorizzati al trattamento e amministratori negligenti
- Fonti umane interne – autorizzati al trattamento e amministratori infedeli
- Fonti umane esterne – segnalanti negligenti o infedeli
- Fonti non umane – guasti tecnici o bug

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

Le misure rilevanti che contribuiscono alla mitigazione del rischio sono indicate a pagina 19 (tipologia integrità).

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

Limitata.

Gli interessati potrebbero sperimentare inconvenienti significativi, superabili nonostante alcune difficoltà.

Eventuali errori (dolosi o colposi) nei dati potrebbero portare a provvedimenti disciplinari o iniziative giudiziarie infondate. Tuttavia – fermo restando che il procedimento stesso può costituire un danno – si tratta di processi caratterizzati da un alto livello di formalizzazione, verifica e tutela, che offrono occasione di rettificare le informazioni non corrette.

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

Trascurabile.

Date le misure di sicurezza tecniche e organizzative adottate, appare quasi impossibile che le fonti di rischio considerate concretizzino una minaccia.

Valutazione: Accettabile

Perdita di dati

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

La perdita di dati potrebbe comportare uno spreco di tempo (qualora il titolare dovesse chiedere all'interessato di trasmettere nuovamente i dati stessi), e potrebbe arrecare disagi (sia al segnalante sia al segnalato) se ne conseguisse un ritardo ingiustificato nella gestione delle segnalazioni.

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

- Cancellazione accidentale dovuta a errore umano
- Cancellazione accidentale dovuta al malfunzionamento dell'infrastruttura IT
- Distruzione accidentale dei supporti ove sono conservati i dati
- Inaccessibilità dei dati conseguente a infezioni ransomware
- Cancellazione dolosa dei dati

Quali sono le fonti di rischio?

- Fonti umane esterne – criminali informatici
- Fonti umane interne – autorizzati al trattamento e amministratori negligenti
- Fonti umane interne – autorizzati al trattamento e amministratori infedeli
- Fonti non umane – incendi, terremoti, alluvioni, altri disastri
- Fonti non umane – guasti tecnici o bug

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

Le misure rilevanti che contribuiscono alla mitigazione del rischio sono indicate a pagina 19 (tipologia disponibilità).

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

Limitata.

Gli interessati potrebbero sperimentare inconvenienti significativi, superabili nonostante alcune difficoltà.

L'impatto di una perdita dei dati è limitato poiché rimediabile acquisendo nuovamente i dati stessi. Le conseguenze negative sono quindi limitate a ritardi o perdite di tempo.

Anche nel caso peggiore di perdita totale dei dati di cui il titolare non sia consapevole, il segnalante può re-inoltrare la segnalazione ai canali esterni (o, a propria discrezione, riproporla internamente).

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

Trascurabile.

Considerate le misure di sicurezza adottate (backup), appare quasi impossibile che le fonti di rischio considerate concretizzino una minaccia.

Valutazione: Accettabile

Misure individuate e mitigazione del rischio

Nella seguente tabella si evidenziano le corrispondenze tra le misure individuate e le tipologie di rischio rispetto alle quali esse svolgono una mitigazione. La presenza di una x nelle colonne Riservatezza (cioè "Accesso illegittimo ai dati"), Integrità (cioè ""Modifiche indesiderate ai dati) o Disponibilità (cioè "Perdita di dati") indica che la misura esercita una mitigazione su quella tipologia di rischio.

Misure individuate		Riservatezza	Integrità	Disponibilità
Ambito	**Misura**	**Accesso illegittimo ai dati**	**Modifiche indesiderate dei dati**	**Perdita di dati**
Misure applicate ai dati	Crittografia	x	x	
Misure applicate ai dati	Anomizzazione	x	x	
Misure applicate ai dati	Controllo degli accessi logici	x	x	
Misure applicate ai dati	Minimizzazione dei dati	x	x	
Misure applicate ai dati	Tracciabilità		x	x
Misure applicate ai dati	Archiviazione		x	x
Misure generali di sicurezza dei sistemi	Gestione delle vulnerabilità	x	x	x
Misure generali di sicurezza dei sistemi	Tracciabilità		x	x
Misure generali di sicurezza dei sistemi	Backup		x	x
Misure generali di sicurezza dei sistemi	Controllo degli accessi fisici	x	x	x
Misure generali di sicurezza dei sistemi	Sicurezza dei canali informatici	x		
Misure generali di sicurezza dei sistemi	Prevenzione delle fonti di rischio umane e non umane		x	x
Misure generali di sicurezza dei sistemi	Gestione postazioni	x		
Misure generali di sicurezza dei sistemi	Lotta contro il malware	x	x	x
Misure generali di sicurezza dei sistemi	Sicurezza dei siti web	x	x	x
Misure generali di sicurezza dei sistemi	Manutenzione	x	x	x
Misure generali di sicurezza dei sistemi	Contratto con il responsabile del trattamento	x	x	x
Misure generali di sicurezza dei sistemi	Sicurezza dell'hardware		x	x
Misure organizzative	Politica di tutela della privacy	x		
Misure organizzative	Gestione delle politiche di tutela della privacy	x		
Misure organizzative	Gestione dei rischi; Vigilanza sulla protezione dei dati	x		
Misure organizzative	Integrare la protezione della privacy nei progetti	x		
Misure organizzative	Gestire gli incidenti di sicurezza e le violazioni dei dati personali; Gestione dei terzi che accedono ai dati	x	x	x
Misure organizzative	Gestione del personale	x	x	x

Panoramica dei rischi

Panoramica

Contesto

Panoramica del trattamento	
Standard applicabili	**Accettabile**
Dati, processi e risorse di supporto	
Categorie dei dati trattati	**Accettabile**
Ciclo di vita dei dati trattati	**Migliorabile**
Risorse di supporto ai dati	**Accettabile**

Principi fondamentali

Proporzionalità e necessità	
Finalità	**Accettabile**
Basi legali	**Accettabile**
Adeguatezza dei dati	**Accettabile**
Esattezza dei dati	**Accettabile**
Periodo di conservazione	**Accettabile**
Misure a tutela dei diritti degli interessati	
Informativa	**Accettabile**
Raccolta del consenso	**Accettabile**
Diritto di accesso e diritto alla portabilità dei dati	**Accettabile**
Diritto di rettifica e diritto di cancellazione	**Accettabile**
Diritto di limitazione e diritto di opposizione?	**Accettabile**
Diritto di non essere sottoposti a trattamento automatizzato	**Accettabile**
Responsabili del trattamento	**Accettabile**
Trasferimenti di dati	**Accettabile**

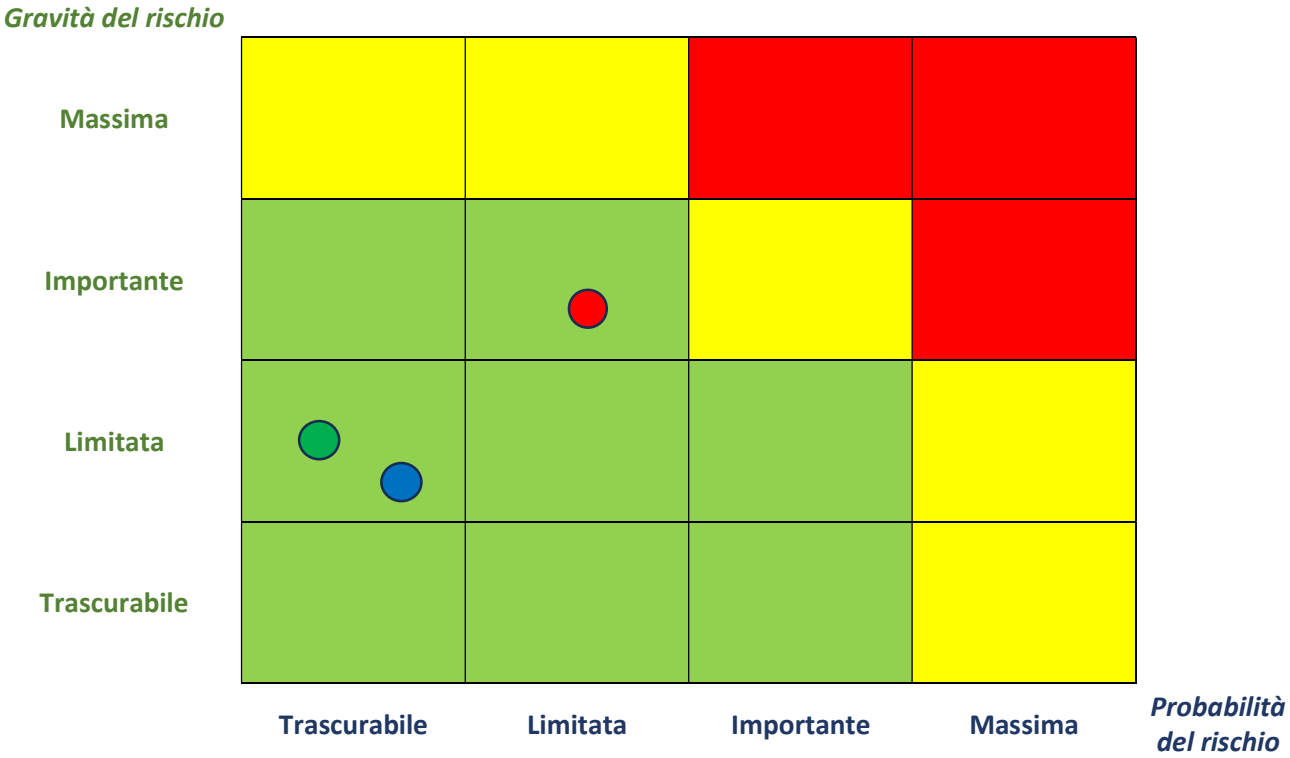
Misure esistenti o pianificate

Misure applicate ai dati	
Crittografia	Accettabile
Anomizzazione	Accettabile
Controllo degli accessi logici	Accettabile
Minimizzazione dei dati	Accettabile
Tracciabilità	Accettabile
Archiviazione	Accettabile
Misure generali di sicurezza dei sistemi	
Gestione delle vulnerabilità	Accettabile
Tracciabilità	Accettabile
Backup	Accettabile
Controllo degli accessi fisici	Accettabile
Sicurezza dei canali informatici	Accettabile
Prevenzione delle fonti di rischio umane e non umane	Accettabile
Gestione postazioni	Migliorabile
Lotta contro il malware	Accettabile
Sicurezza dei siti web	Accettabile
Manutezione	Accettabile
Contratto con il responsabile del trattamento	Accettabile
Sicurezza dell'hardware	Accettabile
Misure organizzative	
Politica di tutela della privacy	Accettabile
Gestione delle politiche di tutela della privacy	Accettabile
Gestione dei rischi; Vigilanza sulla protezione dei dati	Accettabile
Integrare la protezione della privacy nei progetti	Accettabile
Gestire gli incidenti di sicurezza e le violazioni dei dati personali; Gestione dei terzi che accedono ai dati	Accettabile
Gestione del personale	Accettabile

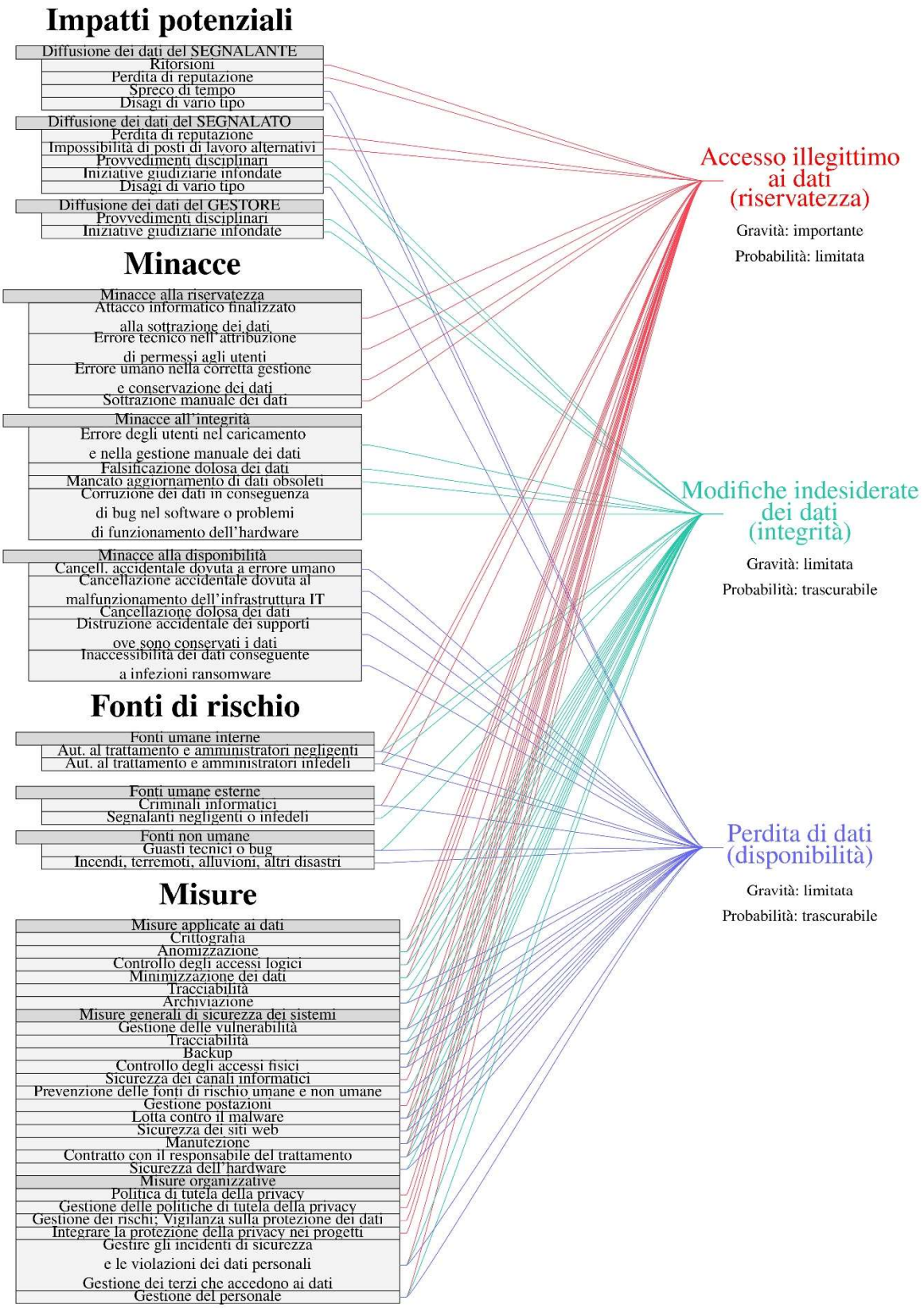
Rischi

Accesso illegittimo ai dati	Accettabile
Modifiche indesiderate dei dati	Accettabile
Perdita di dati	Accettabile

Gravità del rischio



Fattori connessi alla tipologia di violazione



Criticità riscontrate e proposte per azioni correttive

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Valutazione: Migliorabile

Commento di valutazione: attualmente non è possibile effettuare la segnalazione mediante linee telefoniche o sistemi di messaggistica vocale. Resta fermo che il segnalante può concordare un incontro di persona con il gestore ed esporre verbalmente la propria segnalazione in tale sede.

Soluzione proposta: attivare il sistema di registrazione di messaggi vocali disponibile all'interno del software GlobaLeaks.

Gestione postazioni

Valutazione: Migliorabile

Commento di valutazione: le postazioni non sono dotate di un sistema di cifratura del disco locale.

Soluzione proposta: dotare il PC utilizzato dal gestore di strumenti di crittografia del disco locale.

Validazione sulla DPIA

Opinione del DPO e degli interessati sulla DPIA

Nome del DPO

Mattia Cortinovis

Parere del DPO

Il trattamento risulta proporzionato rispetto alle finalità perseguite, è svolto nel rispetto della normativa privacy applicabile, ed è caratterizzato da adeguate misure di sicurezza tecniche ed organizzative.

Con particolare riferimento alle conseguenze di un'eventuale violazione della riservatezza, permangono alcuni rischi inerenti alle caratteristiche del trattamento e alla delicatezza dei dati gestiti. Tali rischi – pur mitigati per quanto possibile – risultano ineliminabili, ma vengono accettati in ragione dell'obbligo legale di procedere all'attività di trattamento.

All'esito della DPIA sono comunque emerse alcune specifiche opportunità di miglioramento. Sul punto si rinvia al paragrafo "Criticità riscontrate e proposte per azioni correttive".

Richiesta del parere degli interessati

Non è stato chiesto direttamente il parere degli interessati. In ogni caso, ai fini dell'attivazione del canale di segnalazione interna, viene fornita idonea informativa alle organizzazioni sindacali.

Motivazione della mancata richiesta del parere degli interessati

Date le caratteristiche specifiche del trattamento e degli interessati, nonché i vincoli imposti dalla normativa in materia di whistleblowing, allo stato l'acquisizione del parere non risulta fattibile.

Copia cartacea per cittadine e cittadini privi di domicilio digitale

(articolo 3-bis, commi 4-bis, 4-ter e 4-quater del decreto legislativo 7 marzo 2005, n. 82)

La presente copia cartacea è tratta dal documento informatico originale, predisposto dall'Amministrazione scrivente in conformità alla normativa vigente e disponibile presso la stessa.
La stampa del presente documento soddisfa gli obblighi di conservazione e di esibizione dei documenti previsti dalla legislazione vigente.

Copia prodotta in data: 11/12/2023

Buongiorno Ilaria,
come da accordi ti allego il documento definitivo (con inseriti i grafici) in formato pdf.
Buona giornata,
Mattia

Dott. Mattia Cortinovis
DATA PROTECTION OFFICER - AREA LEGALE
GRCteam Srl - Gruppo IMteam

mattia.cortinovis@imteam.it
377 1318906
via Sigismondi, 40 - 24018 Villa d'Almè (BG)
grcteam.it

Da: Ilaria Molteni <i.molteni@comune.mariano-comense.co.it>
Inviato: lunedì 11 dicembre 2023 11:06
A: Mattia Cortinovis <mattia.cortinovis@imteam.it>
Oggetto: ok DPIA

Buongiorno Mattia,
la DPIA è stata valutata dalla Segretaria la quale conferma le parti evidenziate in giallo. Puoi dunque cortesemente procedere con l'inserimento dei grafici e l'invio del testo definitivo.
Grazie!

Ilaria Molteni Napoli
Ufficio Appalti, Contratti, Finanziamenti
Settore Affari Generali
Tel. 031/757255
i.molteni@comune.mariano-comense.co.it
appaltiecontratti@comune.mariano-comense.co.it

Copia cartacea per cittadine e cittadini privi di domicilio digitale

(articolo 3-bis, commi 4-bis, 4-ter e 4-quater del decreto legislativo 7 marzo 2005, n. 82)

La presente copia cartacea è tratta dal documento informatico originale, predisposto dall'Amministrazione scrivente in conformità alla normativa vigente e disponibile presso la stessa.
La stampa del presente documento soddisfa gli obblighi di conservazione e di esibizione dei documenti previsti dalla legislazione vigente.

Copia prodotta in data: 11/12/2023