Comune di Verano Brianza

Valutazione d'impatto sulla protezione dei dati ai sensi del regolamento UE 2016/679, in relazione al trattamento di dati effettuato per l'inoltro e la gestione della segnalazione di condotte illecite da parte del whistleblower tramite l'applicativo WhistleblowingPA (D. Lgs. 24/2023, c.d. Whistleblowing)

Sommario

Informazioni sulla DPIA

Nome della valutazione d'impatto

Valutazione di impatto in relazione al trattamento di dati effettuato attraverso l'utilizzo della specifica applicazione "WhistleblowingPA", un software gestionale informatizzato adottato per la gestione delle segnalazioni di Whistleblowing, in adempimento al D. Lgs. 24/2023. Detta applicazione è messa a disposizione dal Titolare Comune di Verano Brianza per l'invio, l'acquisizione e la successiva gestione delle segnalazioni di fatti e condotte illecite e/o irregolari inoltrate dal c.d. whistleblower o segnalante al Responsabile della Prevenzione della Corruzione e della Trasparenza del Comune di Verano Brianza, aventi ad oggetto condotte che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica, rilevate nel contesto lavorativo. La presente Dpia è effettuata ai sensi dell'art. 13 D.lgs. n. 24 del 10 marzo 2023.
.

Nome autore

Segretario Comunale del Comune di Verano Brianza, Dott.ssa Claudia La Rosa

Nome valutatore

SI.net Servizi Informatici, nella persona del Dpo Paolo Tiberi.

Nome validatore

Sindaco pro-tempore del Comune di Verano Brianza, Sig. Samuele Consonni, in qualità di rappresentante del Titolare del Trattamento

Data

08.05.2024

Contesto

Panoramica del trattamento

L'oggetto della presente DPIA è rappresentato dal trattamento dei dati personali forniti dal segnalante, attraverso specifica applicazione messa a disposizione dal Titolare, per la segnalazione di fatti e condotte illecite (c.d. Whistleblowing) al Responsabile della Prevenzione della Corruzione e della Trasparenza del Comune di Verano Brianza (d'ora in poi anche definito RPCT).
Le finalità del trattamento sono rappresentate dalla necessità di consentire:
- al c.d. whistleblower di segnalare in via riservata presunte condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro o di collaborazione;
- al RPCT di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti garantendo la riservatezza del segnalante.
Il trattamento si svolge garantendo la riservatezza sull'identità del segnalante ai sensi di quanto previsto dall'art. 12 del D. Lgs. 24/2023.

Quale è il trattamento in considerazione?

Il trattamento si basa sulla raccolta e gestione dei dati personali che il segnalante comunica (inoltra) al RPCT. La comunicazione (inoltro), in particolare, avviene attraverso l'utilizzo dell'apposita piattaforma informatica WhistleblowingPA (di seguito "Sistema"), utilizzato per la presentazione e gestione di segnalazioni concernenti l'eventuale commissione di condotte rilevanti ai sensi del D. Lgs 24/2023 delle quali l'interessato sia venuto a conoscenza in ragione del proprio rapporto di lavoro o di collaborazione.
In particolare possono essere segnalate attraverso questa applicazione violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica.
Nello specifico, il soggetto che intende effettuare una segnalazione può utilizzare il Sistema per trasmettere informazioni, unitamente a testi e files a supporto della segnalazione, rivolte al RPCT del Titolare. All'arrivo di una segnalazione, il RPCT la prende in carico garantendo la riservatezza dell'identità della persona segnalante, della/e persona/e coinvolta/e e della/e persona/e comunque menzionata/e nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione. Il RPCT, a seguito della segnalazione, può chiedere integrazioni, chiarimenti a supporto della segnalazione, svolgere attività istruttorie di verifica e controllo, anche convocando i soggetti coinvolti, al fine di valutare la sussistenza dei fatti segnalati, unitamente all'esito delle indagini e alle eventuali misure da adottare (ivi compresa l'archiviazione in caso di infondatezza).
Al segnalante, pertanto, viene assegnato un codice univoco, attraverso il quale lo stesso può controllare lo stato di avanzamento/annullamento del procedimento.
Tra segnalante e RPCT viene garantita l'interlocuzione.

Quali sono le responsabilità connesse al trattamento?

Il Titolare del trattamento è il Comune di Verano Brianza.
Whistleblowing Solutions I.S. S.r.l. (da ora in avanti anche definito "Whistleblowing Solutions"), fornitrice del software per la gestione del Whistleblowing, agisce in qualità di responsabile del trattamento. Alcuni suoi operatori operano in qualità di Amministratori di Sistema.
Seeweb, è sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura IaaS.
Transaparency International Italia, è sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing.

Ci sono standard applicabili al trattamento?

Sono applicabili 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
- ISO27018 per la protezione dei dati personali nei servizi Public Cloud
- Qualifica AGID
- Certificazione CSA Star

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Sono effettuate 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.

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

Dati Comuni
Dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

Categorie particolari di dati
Dati eventualmente contenuti nella segnalazione 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.

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

Il ciclo di vita attraverso l'applicativo può essere di seguito riassunto:
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.

Quali sono le risorse di supporto ai dati?

Il trattamento viene effettuato attraverso l'apposita applicazione informatica gestita da Whistleblowing Solutions (Responsabile ex art. 28 GDPR)" basata sulla piattaforma informatica WhistleblowingPA (software GlobaLeaks).
Viene inoltre utilizzata un'infrastruttura IaaS e SaaS privata così strutturata:

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 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 utilizzate 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 version 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.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

I dati forniti dal segnalante al fine di rappresentare le presunte condotte illecite delle quali sia venuto a conoscenza in ragione del proprio rapporto di servizio con l'Ente vengono trattati allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti. Gli scopi perseguiti con il trattamento denominato "Wistleblowing" risultano, in termini generali, leciti, ai sensi dell'art. 5.1.a) Reg. UE 679/2016.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Quali sono le basi legali che rendono lecito il trattamento?

Le basi legali che rendono lecito il trattamento sono: - Necessità del trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, par. 1 lett. e) Reg. UE 679/2016) – Adempimento obblighi di legge (art. 6, par. 1 lett. c) Reg. UE 679/2016)

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

La raccolta dei dati viene effettuata nel rispetto del principio di minimizzazione dei dati, di cui all'art. 5.1 lett. c) Reg. UE 679/2016, ovvero si svolge in maniera tale da ridurre la gravità dei rischi limitando la raccolta di dati personali al minimo necessario per la specifica finalità.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

I dati sono esatti e aggiornati?

Ai sensi dell'art. 5 par. 1 lett. d) Reg. UE 2016/679, i dati trattati sono esatti e, se necessario, aggiornati.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Qual è il periodo di conservazione dei dati?

I dati personali trattati vengono conservati nel rispetto del principio di "limitazione della conservazione" di cui all'art. 5.1 lett. e) Reg. UE 679/2016, in una forma che consenta l'identificazione degli interessati, per un arco di tempo non superiore a 18 mesi.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

L'informativa resa ai soggetti interessati ai sensi dell'art. 13 del Reg. UE 679/2016, è pubblicata sul sito del Comune di Verano Brianza nella sezione Sportello telematico – Segreteria Generale – Segnalare una condotta illecita.
E' presente anche un protocollo operativo, pubblicato nella pagina di accesso al canale, unitamente all'informativa.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Ove applicabile: come si ottiene il consenso degli interessati?

Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità; in caso contrario l'identità della segnalazione non potrà essere rivelata.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

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

L'interessato può richiedere di far valere i Suoi seguenti diritti, nei limiti previsti dall'art. 2-undecies lettera f del D. Lgs. 196/2003, quali:
- accesso ai dati
- rettifica e diritto all'oblio
- limitazione del trattamento
- opposizione al trattamento

a condizione che l'esercizio di tali diritti non comprometta la riservatezza del segnalante.

Valutazione: Accettabile

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

Gli interessati hanno diritto di ottenere la rettifica dei dati personali, nei casi previsti dall'art. 2-undecies lettera f del D. Lgs. 196/2003.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

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

Gli interessati hanno diritto di esercitare i loro diritti di limitazione e di opposizione presentando apposita istanza al Responsabile della prevenzione della corruzione e della trasparenza (R.P.C.T.).

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

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

Sì. Gli obblighi di Wistleblowing Solutions I.S. s.r.l., in qualità di Responsabile del Trattamento, sono definiti nel contratto sottoscritto in data 03.10.2023.

Valutazione: Accettabile
Commento di valutazione: L’analisi effettuata è corretta

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

I dati non vengono trasferiti all’estero.

Valutazione: Accettabile
Commento di valutazione: L’analisi effettuata è corretta

Rischi

Misure esistenti o pianificate

Crittografia

L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington. Il Protocollo crittografico utilizzato è il seguente: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html

Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+.
Ogni informazione sulle segnalazioni - e i relativi metadati registrati 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.
I segnalanti (whistleblowers) accedono alle loro Segnalazioni utilizzando una ricevuta anonima, che è una sequenza di 16 cifre generata casualmente e creata dal Back-End quando la segnalazione viene inviata per la prima volta. La ragione di questo formato di 16 cifre è che assomiglia a un numero di telefono standard, rendendo più facile per i segnalanti nascondere le loro ricevute.

Le password di accesso non vengono mai memorizzate in chiaro ma il sistema mantiene a riposo solo un hash. La piattaforma memorizza le password degli utenti con hash con un salt casuale a 128 bit, unico per ciascun utente. Le password vengono sottoposte ad hashing utilizzando Argon2, una funzione di derivazione chiave che è stata selezionata come vincitrice della Password Hashing Competition nel luglio 2015.

Valutazione; Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Anonimizzazione

L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità di accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.
L'intera applicazione prevede di evitare la registrazione di metadati che potrebbero portare all'identificazione dei segnalanti. I dati sono criptati.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Partizionamento

La componente della segnalazione e la componente che gestisce l'identità sono separati, con accessi diversi gestiti tramite specifica profilazione degli utenti. L'RPCT, per visualizzare l'identità, deve inserire una motivazione e il suo accesso è tracciato.
A livello applicativo, l'identità è disponibile solo a chi ha il ruolo di "Responsabile" nel software. Altrove il segnalante non viene mai indicato con l'identità in chiaro.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

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 il 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.

Il sistema impone l'utilizzo di password complesse implementando un algoritmo personalizzato.

Le password sono classificate in tre livelli: Forte, Accettabile, Insicuro.

Una password classificata al di sotto dei livelli forte o accettabile non è accettata dal sistema.

Il Sistema incoraggia ogni utente finale a utilizzare KeePassXC per generare e conservare password forti e uniche.

Il sistema impone agli utenti di modificare la propria password al primo accesso. Gli amministratori possono anche imporre la modifica della password per gli utenti al successivo accesso.

Per impostazione predefinita, il sistema impone agli utenti di modificare la propria password almeno ogni anno. Questo periodo è configurabile dagli amministratori.

Il sistema richiede a ogni utente una prova su ogni accesso tramite un token o tramite la risoluzione di un problema computazionale prima di poter eseguire un accesso o presentare un invio.

Il sistema implementa altresì il rate limiting, impedendo di eseguire più di 5 richieste di accesso al secondo.
Il sistema identifica poi più tentativi di accesso non riusciti e implementa una procedura di rallentamento in cui un client di autenticazione deve attendere fino a 42 secondi per completare un'autenticazione. Questa funzione ha lo scopo di rallentare possibili attacchi che richiedono più risorse agli utenti in termini di tempo, calcolo e memoria.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Tracciabilità applicata ai dati

L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e una policy di privacy preserving atta a registrare le attività effettuate dagli utenti e dal sistema in conformità al 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.
L'intera applicazione è progettata per cercare di evitare o ridurre le tracce forensi lasciate dai segnalanti sui loro dispositivi durante la compilazione delle loro segnalazioni.
Quando si accede tramite Tor Browser, il browser garantisce che non rimangano tracce persistenti sul dispositivo dell'utente. Al fine di prevenire o limitare le tracce forensi lasciate nella cronologia del browser degli utenti che accedono alla piattaforma tramite un comune browser, l'applicazione evita di modificare l'URI durante la navigazione del whistleblower. Ciò ha l'effetto di impedire al browser di registrare le attività svolte dall'utente e offre un'elevata protezione facendo apparire il whistleblower come un semplice visitatore della home page ed evitando una prova concreta dell'eventuale invio della segnalazione.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Archiviazione

L'applicativo GlobaLeaks implementa un database SQLite integrato, il cui accesso avviene tramite ORM.
Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al controllo da parte dell'applicativo delle funzionalità di sicurezza del database e delle policy di data retention e cancellazione sicura, in aderenza alle raccomandazioni di sicurezza di SQLite (cft https://sqlite.org/security.html)

Valutazione: /Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Sicurezza dei documenti cartacei

I documenti cartacei relativi alle istanze del whistleblowing sono conservati a cura del RPCT in appositi armadi chiusi a chiave.

Valutazione: Migliorabile
Commento di valutazione: si suggerisce di conservare tutto in piattaforma.

Minimizzazione dei dati

Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, E-mail di dell'utente che effettua la registrazione e i dati relativi all'ente (nome, indirizzo, CF e PI).

Sono poi trattati i dati volontariamente rilasciati dal segnalante in merito alla segnalazione. A titolo di esempio:

- se conosciute, le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione;
- descrizione chiara e completa dei fatti oggetto di segnalazione;
- se conosciute, le generalità o altri elementi che consentano di identificare il/i soggetto/i che ha/hanno posto in essere i fatti segnalati;
- l'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;
- allegazione e/o indicazione di eventuali documenti che possono confermare la fondatezza di tali fatti;
- ogni altra informazione e documentazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

Possono altresì essere trattati (Specificare quali dati ulteriori sono trattati):

- le 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 (ad eccezione di quelli relativi al segnalante).
- Dati di registrazione.
- Dati identificativi e di contatto dei soggetti autorizzati dal Titolare alla gestione delle segnalazioni.
- Log di dati identificativi e di contatto dei soggetti autorizzati dal Titolare alla gestione delle segnalazioni.

I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente ai sensi dell'art. 13, comma 2, del d. lgs. 24/2023.

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.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Vulnerabilità

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 (cft Audit di sicurezza: https://docs.globaleaks.org/en/main/security/PenetrationTests.html).
La Web Application Security è implementata dal software in conformità con le OWASP Security Guidelines (cft https://www.owasp.org/).

L'implementazione della sessione segue le linee guida di sicurezza OWASP Session Management Cheat Sheet. (cft https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html)

Il sistema assegna una Sessione a ciascun utente autenticato. L'ID di sessione è lungo 256 bit ed è generato casualmente dal back-end. Ogni sessione scade secondo un time out di 60 minuti. Gli ID di sessione vengono scambiati dal client con il back-end tramite un'intestazione (X-Session) e scadono non appena gli utenti chiudono il browser o la pagina. Gli utenti possono disconnettersi esplicitamente tramite un pulsante di logout o implicitamente chiudendo il browser.

I cookie non vengono utilizzati intenzionalmente per ridurre al minimo gli attacchi XSRF e qualsiasi possibile attacco basato su di essi. Invece di utilizzare i cookie, l'autenticazione si basa su un'intestazione di sessione HTTP personalizzata.
Il sistema implementa un ampio set di intestazioni HTTP appositamente configurate per migliorare la sicurezza del software che ha ottenuto il punteggio A+ da Security Headers e il punteggio A+ da Mozilla Observatory.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Lotta contro il malware

Le postazioni di lavoro del RPCT e dei soggetti designati dispongono di sistemi anti malware aggiornati.
Sono presenti sistemi di sicurezza perimetrale presso la rete del responsabile (Firewall) a protezione dei server.
Tutti i computer del personale di Whistleblowing Solutions e dei suoi Sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale.

L'RPCT è regolarmente nominato e riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware. L'RPCT con utenze del servizio di whistleblowing viene formato e sensibilizzato sulla tematica tramite formazione diretta o documentazione online.
Qualsiasi file allegato dai segnalanti potrebbe contenere un malware che potrebbe essere fornito intenzionalmente o meno. Per scaricare i file in modo sicuro e spostarli utilizzando una chiavetta USB, l'applicazione offre la possibilità di eseguire un'esportazione tramite il download di un archivio ZIP, riducendo la possibilità di eseguire il file con un clic da un dispositivo all'altro.

Valutazione: Accettabile
Commento di valutazione: Valutare se redigere un piano di formazione specifico per l'RPCT.

Gestione postazioni

La postazione di lavoro dell'RPCT è localizzata presso le sedi dell'Ente ed è debitamente messa in sicurezza tramite sistemi anti-malware, aggiornamenti di sistemi operativi e distribuzioni di patch, sistemi di sicurezza perimetrale della rete LAN degli operatori.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Sicurezza dei siti web

Tutte le connessioni sono protette tramite protocollo TLS 1.2+
Le connessioni amministrative privilegiate sono mediate tramite accesso VPN e connessioni con protocollo SSH.
Tutte le segnalazioni vengono inviate tramite SMTP su canale crittografato TLS utilizzando SMTP/TLS o SMTPS, a seconda della configurazione.
Sulla piattaforma vengono tracciati solo cookie tecnici, che sono specificati nella cookie policy.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Backup

I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessario per finalità di disaster recovery.

Valutazione: Migliorabile
Commento di valutazione: specificare se si tratta di policy del comune o del responsabile (dove vanno a finire i dati in back up?)

Manutenzione

La piattaforma utilizzata è una soluzione open source, sviluppata da parte del responsabile per il Titolare, che mette a disposizione un forum di assistenza e di scambio di best practice.

E' prevista manutenzione periodica correttiva, evolutiva e con finalità di assicurare un miglioramento continuo 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 per svolgere le modifiche al sistema e 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 vengono svolte le modifiche al sistema e vengono installati gli aggiornamenti previsti.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Contratto con il responsabile del trattamento

Whistleblowing Solutions, fornitrice dell'Ente per mezzo di adesione ad un contratto di servizio, è stata formalmente nominata dal Titolare come Responsabile del trattamento con uno specifico accordo nel quale viene richiesto al Responsabile di adottare specifiche misure di sicurezza tecniche ed organizzative nel rispetto dell'Art.32 del Regolamento UE 2016 n.679 per tutelare i diritti e le libertà dei soggetti coinvolti nel trattamento.
Nella nomina sono previsti, tra gli altri, i seguenti obblighi:
- l'adozione di misure e procedure tali da garantire la tutela dei dati personali;
- clausole in materia di restituzione e/o distruzione dei dati allo scadere del contratto
- regole per la gestione e la notifica di eventuali incidenti al Titolare.

Il fornitore è stato inoltre designato con funzione di amministratore di sistema.
A sua volta Whistleblowing Solutions ha nominato i propri Sub responsabili del trattamento:
Seeweb, per la gestione dell'infrastruttura (IaaS) e Transparency International Italia, per la collaborazione nella gestione del sistema di whistleblowing.

Valutazione: Migliorabile
Commento di valutazione: Attenzione: Il contratto base prevede limitazioni di responsabilità a favore del fornitore e non prevede servizi manutentivi ad hoc. Si consiglia di provvedere a migliorare detto punto attraverso stipulazione di contratto integrativo ad hoc e/o assicurazioni.

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.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Controllo degli accessi fisici

Il trattamento dei dati viene effettuato in maniera prevalente attraverso l'applicazione informatica.
Per le attività endo-procedimentali e di conservazione ex lege potrebbe essere necessario stampare i documenti: tale documentazione verrebbe conservata in zone ad accesso limitato, e in armadi chiusi a chiave.
Le postazioni e gli armadi si trovano in uffici presidiati accessibili solo da personale autorizzato in orari di lavoro.

Valutazione: Migliorabile
Commento di valutazione: si consiglia di mantenere tutto in piattaforma

Tracciabilità sui sistemi

L’applicativo GlobaLeaks implementa un sistema di audit log sicuro e una policy privacy preserving atta a registrare le attività effettuate dagli utenti.
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.
Sono tracciati anche gli accessi all’applicativo degli incaricati alla gestione della segnalazione.
Sono presenti presso il titolare procedure e sistemi di gestione degli incidenti.

Valutazione: /Accettabile
Commento di valutazione: L’analisi effettuata è corretta

Sicurezza dell’hardware

I dispositivi sono soggetti a misure di sicurezza fisica, essendo situati in zone ad accesso limitato.
I server sono alimentati tramite gruppi di continuità (doppio UPS in parallelo), al fine di proteggerli da sbalzi elettrici.
I datacenter di Seeweb, il fornitore IaaS per conto di Whistleblowing Solutions, dispone 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.

Valutazione: Accettabile
Commento di valutazione: L’analisi effettuata è corretta

Prevenzione delle fonti di rischio

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.

Il backend implementa una rigorosa Content Security Policy (CSP) che impedisce qualsiasi interazione con risorse di terze parti e limita l'esecuzione di input di utenti non attendibili.

Su questa policy predefinita vengono poi implementate policy specifiche in aderenza al principio del privilegio minimo. Ogni input di utente non attendibile o libreria di terze parti viene eseguito in un sandbox che ne limita l'interazione con gli altri componenti dell'applicazione.
Il backend implementa le seguenti policy:

- Cross-Origin-Embedder-Policy (COEP): https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cross-Origin-Embedder-Policy
- Cross-Origin-Opener-Policy (COOP): https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cross-Origin-Opener-Policy
- Cross-Origin-Resource-Policy (CORP): https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy

Valutazione: Accettabile
Commento di valutazione: L’analisi effettuata è corretta

Protezione contro fonti di rischio non umane

Sono presenti le seguenti misure di sicurezza:

- I server sono posizionati in aree a basso rischio sismico ed idrogeologico.
- Separazione di impianti elettrici e batterie in edifici dedicati.
- Impianti monitorati, refrigerati e protetti contro gli incendi.
- I server sono protetti da gruppi di continuità.

Valutazione: /Accettabile
Commento di valutazione: L’analisi effettuata è corretta

Politica di tutela della privacy

Il soggetto responsabile all'interno dell'organizzazione in merito al trattamento dei dati relativo al Whistleblowing è il RPCT, nominato ad hoc autorizzato per questo trattamento.
Il titolare:
- è provvisto di Data Protection Officer, che valuta il presente documento.
- fornisce ai suoi autorizzati e ai Responsabili nominati ex art. 28 GDPR le istruzioni necessarie per trattare i dati personali nel rispetto della normativa in materia di protezione dei dati personali nonché la gestione di eventuali violazioni;
- provvede alla revisione periodica della documentazione tecnica e organizzativa (policy interne), volta ad attuare quanto richiesto dalla normativa, cooperando con gli organi per l'adozione di eventuali modifiche regolamentari o attuative.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Gestione delle politiche di tutela della privacy

È stata adottata una procedura informativa (protocollo) che illustri all'interessato le cautele adottate dal titolare per tutelare i suoi diritti, oltre che le modalità per la presentazione delle segnalazioni.
È prevista una procedura organizzativa, indicata nell'elenco di cui sotto, che prevede gli adempimenti in carico al personale del titolare incaricato.
Il personale è periodicamente formato ed aggiornato sui principi della normativa privacy attraverso sessioni periodiche formative.
Sono state adottate le seguenti procedure:
1) Procedura di gestione del data breach;
2) Procedura di gestione dei soggetti contraenti che trattano dati per conto del Titolare ai sensi dell'art. 28 del Reg. UE 2016/679 - Responsabili del trattamento;
3) Procedura per le autorizzazioni al trattamento dei dati personali ai sensi dell'art 29 Gdpr;
4) Procedura per l'esercizio dei diritti degli interessati, ai sensi degli artt. da 15 a 22 del Reg. UE 2016/679;
5) Procedura per l'elaborazione della valutazione di impatto sulla protezione dei dati (ex art. 35 del Regolamento UE 2016/679).

Valutazione: Migliorabile
Commento di valutazione: indicare le date di approvazione delle procedure indicate.

Gestione dei rischi

L'organizzazione si è dotata di un registro dei trattamenti ai sensi dell'art. 30 RGPD, in cui il trattamento del Whistleblowing è adeguatamente mappato.
L'ente si è dotato di apposite procedure di sicurezza, come ad esempio procedura di gestione dei data breach.
E' stata svolta adeguata formazione.
E' presente un sistema organizzativo interno privacy e la nomina di un dpo.

Valutazione: Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Integrare la protezione della privacy nei progetti

Il titolare si è dotato di un sistema di gestione privacy e nella fase di implementazione del trattamento sia stato coinvolto il DPO.
È stata svolta la presente analisi.

Valutazione: /Accettabile
Commento di valutazione: L'analisi effettuata è corretta

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

L’Ente ha adottato una specifica procedura per la gestione dei data breach; detta procedura individua ruoli e responsabilità connessi al processo di rilevazione, nonché la gestione e la valutazione degli incidenti; la stessa è stata trasmessa a tutto il personale ed è stata svolta specifica formazione.
Ogni incidente è registrato nell’apposito registro di protocollo, in cui sono raccolte le informazioni relative ad ogni evento, gli interventi effettuati e le valutazioni del caso sull’eventuale comunicazione al Garante della Privacy e agli interessati.

Valutazione: Accettabile
Commento di valutazione: L’analisi effettuata è corretta

Gestione del personale

L’RPCT è specificamente autorizzato al trattamento dei dati personali tramite specifiche istruzioni scritte.
Sono note al RPCT tutte le procedure che impattano sulla protezione dei dati.
L’RPCT è formato sui principi della normativa privacy attraverso sessioni formative periodiche.

Valutazione: Accettabile
Commento di valutazione: L’analisi effettuata è corretta

Gestione dei terzi che accedono ai dati

Non sono previsti altri soggetti, ad esclusione del RPCT, che accedono ai dati.
Ai sensi del D. Lgs 23/2024, la segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni.

Valutazione: Accettabile
Commento di valutazione: L’analisi effettuata è corretta

Vigilanza sulla protezione dei dati

La presente DPIA è soggetta a revisione periodica da parte del titolare, in occasione di eventuali variazioni occorse negli strumenti e nei processi di gestione delle segnalazioni.
Il sistema di gestione privacy è monitorato e controllato attraverso audit periodici.
I contratti con i fornitori vengono rinnovati previa verifica delle garanzie necessarie per la protezione dei dati.

Valutazione: /Accettabile
Commento di valutazione: L’analisi effettuata è corretta

Metodo adottato per l'analisi dei rischi

Il modello scelto per quantificare i rischi è quello della misurazione dell'esposizione al rischio:

Esposizione = probabilità x danno

La valutazione del rischio è data dalla combinazione di due parametri, ai quali si attribuisce un valore numerico a seconda della loro valutazione qualitativa. Al fine di oggettivare tale valutazione, si è adottata la metrica proposta da ENISA nel documento "Handbook on Security of Personal Data Processing":

- **gravità del rischio**, intesa come possibile effetto sulla dignità e libertà degli interessati oppure danni materiali agli stessi derivanti dal verificarsi dell'evento considerato a rischio (la gravità del rischio può essere Bassa [1], Media [2], Alta [3], Significativa [4]). I 4 livelli di impatto si possono così descrivere:
  - Bassa [1]: Le persone possono incontrare alcuni piccoli inconvenienti, che supereranno senza problemi (tempo speso per reinserire le informazioni, fastidi, irritazioni, ecc.).
  - Media [2]: Gli individui possono incontrare notevoli inconvenienti, che saranno in grado di superare nonostante alcune difficoltà (costi extra, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).
  - Alta [3]: Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento nella lista nera da parte di istituzioni finanziarie, danni alla proprietà, perdita del lavoro, mandato di comparizione, peggioramento della salute, ecc.).
  - Significativa [4]: Gli Individui possono subire conseguenze significative o addirittura irreversibili, che potrebbero non superare (incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, ecc.).
- **probabilità di accadimento** della minaccia rilevata, sulla base della natura delle minacce, delle fonti di rischio e delle misure esistenti o pianificate (la probabilità può essere Improbabile [1], Bassa [2], Media [3], Alta [4]). I 4 livelli di probabilità di accadimento si possono così descrivere:
  - Improbabile [1]: Appare impossibile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Bassa [2]: Appare difficile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Media [3]: Appare possibile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Alta [4]: Appare estremamente probabile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.

Viene pertanto identificata l'esposizione al rischio, intesa come combinazione moltiplicativa dei due fattori, da cui vengono stabilite le azioni da compiere sulla base della seguente tabella:

Probabilità	Alta	4	4	8	12	16
	Media	3	3	6	9	12
	Bassa	2	2	4	6	8
	Improbabile	1	1	2	3	4
			1	2	3	4
			Bassa	Media	Alta	Significativa
			Gravità			

Le azioni consequenziali da intraprendere sono le seguenti:

Livello di esposizione	Intervallo di valori	Intervento previsto
Minimo	1-3	Da Monitorare
Medio	4-8	Implementare le misure previste entro l'anno
Significativo	9-16	Intervento urgente

Accesso illegittimo ai dati

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

Vendetta, malevolenza, e ritorsioni.
Mancato esercizio di un diritto

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Fonti umane interne ed esterne.

Quali sono le fonti di rischio?

- fonti umane interne: dipendenti che compiono azioni involontarie o fraudolente per motivi di confusione, errore, negligenza, vendetta, volontà di provocare allarme, malevolenza, possibilità di lucro, spionaggio.
- fonti umane esterne: 1) un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo; 2) un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine; 3) una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni. Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento)

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Tracciabilità, Partizionamento, Archiviazione, Sicurezza dei documenti cartacei, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Sicurezza dei siti web, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Prevenzione delle fonti di rischio, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestione dei rischi, Integrare la protezione della privacy nei progetti, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Gestione dei terzi che accedono ai dati, Vigilanza sulla protezione dei dati, Crittografia

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

Significativa

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

Improbabile

Livello di esposizione al rischio

GRAVITA'	PROBABILITA'	ESPOSIZIONE	INTERVENTO PREVISTO
4	1	4	

Valutazione: Accettabile
Commento di valutazione: l'analisi è corretta.

Modifiche indesiderate dei dati

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

Vendetta, malevolenza, e ritorsioni.
Mancato esercizio di un diritto

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

Fonti umane interne ed esterne.

Quali sono le fonti di rischio?

- fonti umane interne: dipendenti che compiono azioni involontarie o fraudolente per motivi di confusione, errore, negligenza, vendetta, volontà di provocare allarme, malevolenza, possibilità di lucro, spionaggio.
- fonti umane esterne: 1) un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo; 2) un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine; 3) una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni. Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento)

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

Controllo degli accessi logici, Tracciabilità, Partizionamento, Archiviazione, Sicurezza dei documenti cartacei, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Sicurezza dei siti web, Backup, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Prevenzione delle fonti di rischio, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestione dei rischi, Integrare la protezione della privacy nei progetti, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Gestione dei terzi che accedono ai dati, Vigilanza sulla protezione dei dati, Crittografia

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

Significativa

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

Improbabile

Livello di esposizione al rischio

GRAVITA'	PROBABILITA'	ESPOSIZIONE	INTERVENTO PREVISTO
4	1	4	

Valutazione: Accettabile
Commento di valutazione: l'analisi è corretta

Perdita di dati

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

Mancato esercizio di un diritto

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

Fonti umane interne, esterne e non umane.

Quali sono le fonti di rischio?

- fonti umane interne: dipendenti che compiono azioni involontarie o fraudolente per motivi di confusione, errore, negligenza, vendetta, volontà di provocare allarme, malevolenza, possibilità di lucro, spionaggio.
- fonti umane esterne: 1) un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo; 2) un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine; 3) una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni. Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento)
- fonti non umane: un incidente o un sinistro (interruzioni di corrente, incendio, inondazione, ecc.).

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

Controllo degli accessi logici, Tracciabilità, Partizionamento, Archiviazione, Sicurezza dei documenti cartacei, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Sicurezza dei siti web, Backup, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Prevenzione delle fonti di rischio, Protezione contro fonti di rischio non umane, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestione dei rischi, Integrare la protezione della privacy nei progetti, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Gestione dei terzi che accedono ai dati, Vigilanza sulla protezione dei dati, Crittografia

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

Significativa

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

Bassa

Livello di esposizione al rischio

GRAVITA'	PROBABILITA'	ESPOSIZIONE	INTERVENTO PREVISTO
4	1	4	

Valutazione: Accettabile
Commento di valutazione: l'analisi dei rischi è corretta

Piano d’azione

Principi fondamentali

ACC	MIG	ELENCO PRINCIPI
X		Finalità
X		Basi legali
X		Adeguatezza dei dati
X		Esattezza dei dati
X		Periodo di conservazione
X		Informativa
X		Raccolta del consenso (sebbene non sia richiesto perché rientrante nelle finalità di pubblico interesse come previsto dall’art. 6 par. 1 lett. e) del GDPR)
X		Diritto di accesso e portabilità dei dati
X		Diritto di rettifica e diritto di cancellazione (ove compatibili il perseguimento delle finalità di pubblico interesse come previsto dall’art. 6 par. 1 lett. e), del GDPR)
X		Diritto di limitazione e diritto di opposizione (ove compatibili finalità di pubblico interesse come previsto dall’art. 6 par. 1 lett. e), del GDPR)
X		Responsabili del trattamento
X		Trasferimenti di dati

ACC: Principi valutati Accettabili
MIG: Principi valutati Migliorabili

Piano d’azione

Trasferimenti di dati: integrare informativa privacy

Misure esistenti e pianificate

ACC	MIG	ELENCO MISURE
X		Crittografia
X		Anonimizzazione
X		Partizionamento
X		Controllo degli accessi logici
X		Tracciabilità applicata ai dati
X		Archiviazione
	X	Sicurezza dei documenti cartacei
X		Minimizzazione dei dati
X		Vulnerabilità
X		Lotta contro il malware
X		Gestione postazioni
X		Sicurezza dei siti web
	X	Backup
X		Manutenzione
	X	Contratto con il responsabile del trattamento
X		Sicurezza dei canali informatici
	X	Controllo degli accessi fisici
X		Tracciabilità sui sistemi
X		Sicurezza dell'hardware
X		Prevenzione delle fonti di rischio
X		Protezione contro fonti di rischio non umane
X		Politica di tutela della privacy
	X	Gestione delle politiche di tutela della privacy
X		Gestione dei rischi
X		Integrare la protezione della privacy nei progetti
X		Gestire gli incidenti di sicurezza e le violazioni dei dati personali
X		Gestione del personale
X		Gestione dei terzi che accedono ai dati
X		Vigilanza sulla protezione dei dati

ACC: Misure valutate Accettabili

MIG: Misure valutate Migliorabili

Piano d'azione

Non previsto

Rischi

ACC	MIG	ELENCO RISCHI
X		Accesso illegittimo ai dati
X		Modifiche indesiderate dei dati
X		Perdita dei dati

ACC: Principi valutati Accettabili
MIG: Principi valutati Migliorabili

Piano d'azione

Non previsto

Pareri

Parere DPO/RPD

Paolo Tiberi, nella qualità di Responsabile Protezione Dati del comune di Verano Brianza, ha espresso il seguente parere:
Il trattamento può essere implementato

Si richiede tuttavia di implementare gli aspetti di miglioramento e risolvere le criticità segnalate entro sei mesi

Parere degli interessati

Non è stato chiesto il parere degli interessati in quanto non necessario, poiché la base legale del trattamento è costituita dall'adempimento, ex art. 6, comma 1, lett. c) del GDPR, cioè adempiere a un obbligo legale al quale è soggetto il titolare del trattamento.